

# FEDERAL AGENCY PROTECTION OF PRIVACY ACT

---

HEARING  
BEFORE THE  
SUBCOMMITTEE ON  
COMMERCIAL AND ADMINISTRATIVE LAW  
OF THE  
COMMITTEE ON THE JUDICIARY  
HOUSE OF REPRESENTATIVES  
ONE HUNDRED SEVENTH CONGRESS  
SECOND SESSION

ON

**H.R. 4561**

MAY 1, 2002

**Serial No. 80**

Printed for the use of the Committee on the Judiciary



Available via the World Wide Web: <http://www.house.gov/judiciary>

U.S. GOVERNMENT PRINTING OFFICE

79-365 PDF

WASHINGTON : 2002

---

For sale by the Superintendent of Documents, U.S. Government Printing Office  
Internet: [bookstore.gpo.gov](http://bookstore.gpo.gov) Phone: toll free (866) 512-1800; DC area (202) 512-1800  
Fax: (202) 512-2250 Mail: Stop SSOP, Washington, DC 20402-0001

## COMMITTEE ON THE JUDICIARY

F. JAMES SENSENBRENNER, JR., WISCONSIN, *Chairman*

HENRY J. HYDE, Illinois	JOHN CONYERS, JR., Michigan
GEORGE W. GEKAS, Pennsylvania	BARNEY FRANK, Massachusetts
HOWARD COBLE, North Carolina	HOWARD L. BERMAN, California
LAMAR SMITH, Texas	RICK BOUCHER, Virginia
ELTON GALLEGLY, California	JERROLD NADLER, New York
BOB GOODLATTE, Virginia	ROBERT C. SCOTT, Virginia
ED BRYANT, Tennessee	MELVIN L. WATT, North Carolina
STEVE CHABOT, Ohio	ZOE LOFGREN, California
BOB BARR, Georgia	SHEILA JACKSON LEE, Texas
WILLIAM L. JENKINS, Tennessee	MAXINE WATERS, California
CHRIS CANNON, Utah	MARTIN T. MEEHAN, Massachusetts
LINDSEY O. GRAHAM, South Carolina	WILLIAM D. DELAHUNT, Massachusetts
SPENCER BACHUS, Alabama	ROBERT WEXLER, Florida
JOHN N. HOSTETTLER, Indiana	TAMMY BALDWIN, Wisconsin
MARK GREEN, Wisconsin	ANTHONY D. WEINER, New York
RIC KELLER, Florida	ADAM B. SCHIFF, California
DARRELL E. ISSA, California	
MELISSA A. HART, Pennsylvania	
JEFF FLAKE, Arizona	
MIKE PENCE, Indiana	

PHILIP G. KIKO, *Chief of Staff-General Counsel*

PERRY H. APELBAUM, *Minority Chief Counsel*

---

## SUBCOMMITTEE ON COMMERCIAL AND ADMINISTRATIVE LAW

BOB BARR, Georgia, *Chairman*

JEFF FLAKE, Arizona, <i>Vice Chair</i>	MELVIN L. WATT, North Carolina
GEORGE W. GEKAS, Pennsylvania	JERROLD NADLER, New York
MARK GREEN, Wisconsin	TAMMY BALDWIN, Wisconsin
DARRELL E. ISSA, California	ANTHONY D. WEINER, New York
STEVE CHABOT, Ohio	MAXINE WATERS, California
MELISSA HART, Pennsylvania	

RAYMOND V. SMJETANKA, *Chief Counsel*

SUSAN JENSEN-CONKLIN, *Counsel*

ROBERT NEIRA TRACCI, *Full Committee Counsel*

PATRICIA DEMARCO, *Full Committee Counsel*

STEPHANIE MOORE, *Minority Counsel*

# CONTENTS

MAY 1, 2002

## OPENING STATEMENT

	Page
The Honorable Bob Barr, a Representative in Congress From the State of Georgia, and Chairman, Subcommittee on Commercial and Administrative Law .....	1
The Honorable Melvin L. Watt, a Representative in Congress From the State of North Carolina, and Ranking Member, Subcommittee on Commercial and Administrative Law .....	3
The Honorable Jerrold Nadler, a Representative in Congress From the State of New York .....	5
The Honorable Mark Green, a Representative in Congress From the State of Wisconsin .....	5
The Honorable Steve Chabot, a Representative in Congress From the State of Ohio .....	6
The Honorable George W. Gekas, a Representative in Congress From the State of Pennsylvania .....	7

## WITNESSES

Ms. Lori L. Waters, Executive Director, Eagle Forum	
Oral Testimony .....	9
Prepared Statement .....	11
Mr. Gregory T. Nojeim, Associate Director and Chief Legislation Counsel, American Civil Liberties Union	
Oral Testimony .....	13
Prepared Statement .....	14
Mr. James Harper, Editor, Privacilla.org, and Adjunct Fellow, Progress and Freedom Foundation	
Oral Testimony .....	19
Prepared Statement .....	21
Mr. Edmund Mierzwinski, Consumer Program Director, United States Public Interest Research Group	
Oral Testimony .....	27
Prepared Statement .....	28

## APPENDIX

### MATERIAL SUBMITTED FOR THE HEARING RECORD

Post-Hearing Questions and Answers from Congressman Bob Barr to Mr. Gregory Nojeim, Associate Director and Chief Legislative Counsel, American Civil Liberties Union .....	43
Post-Hearing Questions and Answers from Congressman Bob Barr to Mr. James Harper, Editor, Privacilla.org, and Adjunct Fellow, Progress and Freedom Foundation .....	48



## FEDERAL AGENCY PROTECTION OF PRIVACY ACT

---

WEDNESDAY, MAY 1, 2002

HOUSE OF REPRESENTATIVES,  
SUBCOMMITTEE ON COMMERCIAL  
AND ADMINISTRATIVE LAW,  
COMMITTEE ON THE JUDICIARY,  
*Washington, DC.*

The Subcommittee met, pursuant to notice, at 10:18 a.m., in Room 2141, Rayburn House Office Building, Hon. Bob Barr [Chairman of the Subcommittee] presiding.

Mr. BARR. Good morning. I would like to convene this hearing of the Subcommittee on Commercial and Administrative Law to receive testimony on pending legislation, H.R. 4561, the Federal Agency Protection of Privacy Act. We will at this time call the Subcommittee to order.

We meet this morning to receive testimony on H.R. 4561, the Federal Agency Protection of Privacy Act, legislation which I have introduced with the bipartisan cosponsorship of several Members of the Subcommittee, including the distinguished Ranking Member, Mr. Mel Watt, of the great State of North Carolina.

I am grateful for the cosponsorship of so many Members of the Subcommittee and others, but particularly that of Mr. Watt. We have worked cooperatively on a number of issues before the Subcommittee and I hope we can together speedily send this "good government" initiative on its way through the House and ultimately to the President's desk.

It is clear that those of us who support this legislation do not agree on every issue. In fact, many observers have been particularly impressed by the political diversity of the bill's cosponsors, two of which are here with us today on my left, Mr. Watt and Mr. Nadler, whom we appreciate very much lending their tremendous prestige and background on privacy matters to this legislation. I am also pleased to welcome a distinguished panel which also spans the conventional ideological spectrum.

Supporters of this legislation share a commitment to protecting the privacy cherished by American citizens that is at the core of our society, a value increasingly imperiled in an information age in which personal information has become a commodity that is captured, compiled, manipulated, misused, bought and sold in ways not imagined even a few years ago.

The sphere of privacy which Justice Brandeis eloquently described as "the right to be left alone" is not only rapidly diminishing, it is increasingly penetrable. Special care is necessary to en-

sure that personal information remains personal, absent a very sound and lawful reason to treat it otherwise. This value is neither exclusively Republican nor Democrat, liberal nor conservative. It is a truly American value.

H.R. 4561 takes the first necessary step toward protecting the privacy of information collected by the Federal Government. While some have decried the loss of personal privacy by private companies, it must be emphasized that Government alone has the authority to compel the disclosure of personal information, and unlike a private commercial gatherer of personal data, the Government can put you in jail based on what it uncovers. For this reason, the Government has an obligation to exercise greater responsibility when enacting policies that undermine privacy rights.

The Federal Agency Protection of Privacy Act requires that rules noticed for public comment by Federal agencies be accompanied by an assessment of the rule's impact on personal privacy interests, including the extent to which the proposed rule provides notice of the collection of personally identifiable information, what information will be obtained, and how it is to be collected, maintained, used, and disclosed.

The measure further provides that final rules be accompanied by a final privacy impact analysis which indicates how the issuing agency considered and responded to privacy concerns raised by the public and explains whether the privacy—whether the agency could have taken an approach less burdensome to personal privacy.

Unlike existing laws that protect against the disclosure of information already obtained by the Federal Government, the Federal Agency Protection of Privacy Act requires prospective notice of a proposed rule's effect on privacy before it becomes a binding regulation.

An earlier version of this measure was introduced last Congress by Representative Steve Chabot, a very distinguished Member of this Subcommittee and the Chairman of the Judiciary Subcommittee on the Constitution, and we appreciate his work both in the last Congress and in this Congress on this important legislative initiative.

H.R. 4561 specifically articulates the principles that should guide agency action when rules that impact privacy are promulgated. One, the public should have notice that a rule provides for the collection of personally identifiable information and how the agency will collect, maintain, use, and disclose that information.

Two, individuals should have access to information that pertains to them and an opportunity to correct inaccuracies.

Three, agencies should take steps to prevent information collected for one purpose from being used for another purpose.

And, four, agencies should take steps to provide security for such information.

Importantly, H.R. 4561 permits individuals who are adversely affected by an agency's failure to follow its provisions to seek judicial review pursuant to the provisions of the Administrative Procedure Act. In this respect, the bill tracks the administrative innovations of 1996 amendments to the Regulatory Flexibility Act, which provided for judicial review of rules issued without regard to their impact on small businesses. I can say without hesitation that privacy

is no less important to American citizens than regulatory burdens are to American businesses, and this measure we are considering today significantly helps address those concerns.

Finally, I want to emphasize that H.R. 4561 will not unduly burden regulators, nor will it hinder or hamper law enforcement activities. The Federal Agency Protection of Privacy Act will apply the best antiseptic—sunshine—to the Federal rulemaking process by securing the public's right to know about how rules will affect their personal privacy, while ensuring that citizens have the opportunity not only to critique the substance of a rule, but to do so with an understanding of the reasoning and justification upon which the rule was predicated.

I now yield to the distinguished Ranking Member from North Carolina for his opening remarks.

Mr. WATT. Thank you, Mr. Chairman, and I thank the witnesses first for being here to testify about this proposed legislation, and look forward to their testimony, and thank the Chairman for convening this hearing. This is probably a record. It seems like it was just last week that we were having a press conference in preparation for dropping or introducing this bill.

He got it introduced, referred to the Committee, referred to the Subcommittee, and is having a hearing in record time, I suspect. So I have to marvel at the power of my Chairman and compliment him on that, and the speed of my Chairman.

Mr. BARR. Flattery will get you a great deal in this business. Thank you.

Mr. WATT. Always when I am on your side, I flatter you.

I was thinking, you know, the longer I stay in this business, the more I understand that much of what we do involves a tug of war between how much Government does and how much the private individual does. We have a perpetual debate about the amount that we tax so that the Government can do things, or the amount that we don't tax so that Government can't afford to do things.

We have a perpetual battle between the rights of Government to exercise police power, or the amount that they do not exercise police power, and that balance fortunately is articulated pretty well in the fourth amendment and some of the other amendments to the Constitution.

And this is yet another one of those tugs of wars that we are perpetually involved in. How much information should our Government collect about individuals, and what rights should individuals have to protect themselves and maintain their privacy and keep their Government out of their lives, to be not interfered with? And it strikes me that this bill is a rather ingenious way to resolve that tug of war.

We don't really have an independent commission to kind of look at the tax-and-spend balance that we have. We have to do it pretty much ourselves. We don't have an independent body, except for the courts after the fact to strike the appropriate balance between criminal defendants and the Government.

Here, we have an opportunity to require Government agencies to evaluate what they are doing in terms of invasion of privacy so that they inform the public about what implications what they are

doing and the information they are collecting will have on their privacy rights.

It makes the—this bill would make Government agencies think about and articulate what the appropriate balance should be, and it would empower individual citizens with information to make them think about and evaluate what that balance should be. This is a very ingenious approach to solving this problem because we are not saying that the Government can't collect information. What we are saying is if it does, it should do so in a well-thought-out, well-reasoned way, in a justifiable, defensible way, and in a way that has the minimum impact that it can have on the individual rights of citizens in our country.

And it should articulate that rationale and those reasons, and assure the public it has thought about the least intrusive way to accomplish the governmental objective that we have outlined in legislation or in regulations as we go forward.

So I like this bill. And, of course, when I like a bill, I cosponsor it. It is really not about this being a Republican bill or a Democratic bill. It is not about it being a conservative bill or a liberal bill. In fact, I think what we normally find in the privacy context and in a number of contexts where we are trying to draw this line between the appropriate role of Government and the appropriate role of individuals is the extremes that really coalesce around protection of individual liberties.

The people in the middle tend to never think that the Government will kick their doors in inappropriately and search and seize their property, or collect information about them that is inappropriate. They give the Government that presumption that whatever the Government does is an appropriate Government role.

People who are expressing themselves either on the right or on the left, or not necessarily in the mainstream on issues whether they are on the right or the left, are concerned about maintaining the right to individual liberties in this country, and so it is a natural coalition.

I talked at the press conference about quite often backing around the circle and running into my colleague on the Senate side, Jesse Helms. We do that quite often, and typically it is in the area either of individual rights, such as this bill would protect, or some interest that is unique to North Carolina. Those two things we find ourselves meeting each other on, and it is great to be able to work with my Chairman on this bill and I hope we can correct whatever concerns the witnesses can identify about it, amend it, make it better, move it on to the full Committee, get it to the floor and get it to the President's desk for signature as soon as possible.

I thank the gentleman for yielding time and I yield back.

Mr. BARR. I thank the gentleman, the distinguished Ranking Member, for his eloquence.

I would now like to recognize the distinguished Vice Chairman of the Committee, the gentleman from Arizona, Mr. Flake, for any opening statement he might have.

Mr. FLAKE. Thank you, Mr. Chairman. I have no opening statement. I just look forward to hearing the witnesses. Thanks.



Mr. BARR. I thank the gentleman from Arizona for his great eloquence and recognize the distinguished gentleman from New York, Mr. Nadler, a true champion of privacy.

Mr. NADLER. Thank you, sir. I want to commend the Chairman of the Subcommittee for taking initiative in introducing this bill, and also for holding this hearing, as the Ranking Minority Member noted, with great dispatch.

I support and cosponsor the Federal Agency Protection of Privacy Act, which essentially calls on Federal agencies to include privacy impact analyses with proposed regulations, and I look forward to the hearing this morning.

It is time for the Federal Government to take privacy seriously and to consider the impact of the rules and regulations on the privacy rights of every American. At a time when personal information can be stored and accessed so easily by electronic means, it is more important than ever to take steps to safeguard the privacy of average Americans.

And when personal information is often the key to unlocking modern services and paying for them, it is critical that we limit access to private personal information and prevent the Government from inadvertently sharing that information with others.

Even in this time of enhanced fears of terrorist attacks, it is important that the individual liberties of our citizens not be sacrificed to the war on terrorism. We can have both liberty and safety. We can have both privacy and security. That is the entire purpose of this country. We just have to strike the proper balance between the two. This bill is designed to help us make those decisions by accurately assessing the privacy impact of Federal regulations.

Keep in mind, nothing in this bill prohibits agencies from taking actions that may at times sacrifice privacy for the greater good. What the bill will do is clearly inform the public and the decision-makers of the implications for privacy rights of certain proposed laws and regulations.

The legislation mandates the production of privacy reports. The public, as well as the decisionmakers, will have a chance to review these reports and decide if the policy or program is worth sacrificing whatever privacy rights of individuals may be at stake in those regulations.

Fundamentally, this bill is about education. It is about educating the public about their rights to privacy and helping them make informed decisions based on that information. That is why I am pleased to support the bill, and again I thank the Chairman.

Thank you very much, and I yield back.

Mr. BARR. I thank the distinguished gentleman from New York and recognize the distinguished gentleman from Wisconsin, Mr. Green, for any opening statement he might have.

Mr. GREEN. Thank you, Mr. Chairman. Very briefly, this legislation won't change the world, obviously. As you have pointed out, it is not burdensome upon agencies, but what it will do is arm us as policymakers and legislators with information. We can choose to ignore it, we can choose to do whatever we will do with respect to legislation and rules, but at least none of us will be able to argue that we didn't know what the impact would be. And I think that legislation that creates tools like that is vitally important to us

doing our work. I would wish that we would do that on more fronts than simply on privacy.

For me, this issue came home very sharply during our consideration of the bankruptcy legislation, when we discovered in the debate on bankruptcy in the Judiciary Committee that there were a number of longstanding recordkeeping requirements that in the past didn't seem to have great significance because, in practice, for people to get the information they would have to go to the courthouse and they would have to go to the desk and file a written request and sort through globs of information before they could find out the details.

But now that this information is being stored electronically and now that it can be sorted electronically, it was stunning the information that was revealed. In one case, I discovered that in listing the debtor, they also listed the names, ages, and locations of all the minor children.

Now, I am not sure that is information that we would particularly like to be available out there for anybody to get through a simple push of a button. So for me, that just reminded me that information which in the past would have been hard to access all of a sudden is amazingly easy to access, and obviously it is incumbent upon us to take steps to protect it. I think this legislation is a small step toward doing that, and I yield back my time and thanks for the opportunity to make a statement.

Mr. BARR. I thank the distinguished gentleman from Wisconsin.

I would like to now recognize the very distinguished gentleman from Ohio, Mr. Chabot, the Chairman of the Constitution Subcommittee, who in the last Congress especially took the lead on bringing this important matter to the forefront and is a vital player in our efforts in this Congress to continue this work.

The gentleman from Ohio is recognized.

Mr. CHABOT. Thank you, Mr. Chairman, and I want to thank the Chairman for his leadership in introducing this important privacy rights legislation and holding this hearing, as Mr. Watt said, in record time. And so I want to compliment him for this. And thanks for the recognition in having introduced this myself last—or something very similar last Congress.

And the reason I did that is because I think too often privacy rights have become what amounts to an after-thought in the regulatory process. We have seen attempt after attempt by the Federal Government and Federal agencies to implement ominous regulations that allow the Government to invade the privacy of American citizens.

From financial information to medical records, the Federal Government has sought access to highly sensitive information without regard to the privacy implications. If enacted, the Federal Agency Protection of Privacy Act will force Federal agencies to open their eyes to legitimate privacy concerns. For the first time, all Federal agencies will be required to assess the privacy implications of proposed rules or regulations, this providing privacy rights of all Americans the full consideration and attention that they deserve.

This legislation is particularly poignant, I believe, at this time. In the wake of the events of September 11, Congress acted promptly to provide law enforcement with the tools that they needed to

effectively fight terrorism. If implemented incorrectly or without regard to privacy concerns, however, some of those tools could have an adverse impact on privacy rights, making it essential for Federal agencies to provide thoughtful consideration from a privacy perspective.

I am proud to cosponsor this vital legislation, and again I want to thank the Chairman and commend him for holding this hearing today and moving forward, and I look forward to hearing the testimony from the witnesses.

I yield back the balance of my time.

Mr. BARR. I thank the distinguished gentleman from Ohio.

We have been joined by another very distinguished Member of this panel, the former Chairman of this Subcommittee, the distinguished gentleman from the Commonwealth of Pennsylvania, Mr. Gekas, who is now recognized for any opening statement he might have.

Mr. GEKAS. I thank the Chair. I am pleased to see Jim Harper is one of the individuals who will be testifying. He will recall that during our battles on attempting to bring about regulatory reform after the new Congress of 1995, et cetera, that one of the elements that we accented there was judicial review as being absent from the normal businessman's visions of what he could do in the furtherance of his enterprise.

So we brought into the consciousness of the Congress a need that this affected consumer or business person would have access to the courts if he found that he was being unjustly treated. Judicial review, as I look at the legislation before us, is also present in this circumstance, and when the time comes for questioning I would like some commentary from everybody, especially Mr. Harper.

Thank you.

Mr. BARR. I thank the gentleman from Pennsylvania.

At this point, there being no additional Members for opening statements, I would like to welcome on behalf of the entire Subcommittee and the entire Judiciary Committee, of which this Subcommittee is a part, the very distinguished panel of four witnesses that we have today.

In preparing for this hearing and in talking with the staff, there is no greater—there is no better panel that we could have had than the four folks with us here today. They all have vast experience and a very, very deep commitment of and understanding of the need to protect privacy in all of its parts, but particularly with regard to intrusions by the Federal Government. So we are very appreciative to the witnesses for being here today, taking time from very, very busy schedules to share their thoughts and answer questions so that we can gather the information that we need to move this legislation forward as quickly as possible.

Our first witness today will be Ms. Lori Waters, who currently serves as the executive director at the Eagle Forum. Prior to being appointed to that position, Ms. Waters served as Eagle Forum's Collegians national director to encourage political activism among America's university students.

Ms. Waters is a prominent spokesperson for issues affecting America's families and has been a guest on many national radio and television programs. She has been an eloquent proponent of

privacy rights and has written several articles concerning Government threats to privacy, including medical privacy regulations. Ms. Waters is a cum laude graduate of Furman University. In Georgia, instead of Latin, we say she done good.

Ms. Waters, we are very happy to have you with us today.

Ms. WATERS. Thank you.

Mr. BARR. Greg Nojeim is our second witness, associate director and chief legislative counsel for the American Civil Liberties Union. Prior to obtaining this distinguished position, Mr. Nojeim was the ACLU's legislative counsel on privacy issues, a capacity in which he was responsible for analyzing the civil liberties implications of Federal legislation relating to information privacy, national security, and immigration.

He has testified before Congress on many occasions and is nationally recognized as a leading privacy advocate. Prior to joining the ACLU, Mr. Nojeim was the Director of Legal Services of the American Arab Anti-Discrimination Committee, or ADC. Mr. Nojeim is a graduate of the University of Rochester and the University of Virginia Law School.

I would like to say it has been a personal pleasure of mine since being in the Congress the last 8 years to have worked with Mr. Nojeim and his compatriots at the ACLU on a number of issues, and I have always found them to be extremely knowledgeable and honest in dealing with us, and look forward to continuing that very productive relationship.

We appreciate your being with us today, Greg.

Our third witness, as the former Chairman and the distinguished gentleman from the Commonwealth of Pennsylvania mentioned, is no stranger to either this panel or these issues. James Harper is editor of Privacilla.org, an Internet-based privacy resource that reflects a free-market stance toward privacy issues.

Mr. Harper also serves as Adjunct Fellow at the Progress and Freedom Foundation, and is a founder and principal of PolicyCounsel.com. Prior to joining Privacilla.org, Mr. Harper held a number of public policy positions, serving as counsel to the U.S. House Judiciary Committee, counsel to the Senate Government Affairs Committee, and as a legal fellow for the Senate Judiciary Committee.

Mr. Harper has written several comprehensive reports on Government privacy, and testified before the House Transportation Committee on the increasing use of red light cameras. He is a graduate of the University of California at Santa Barbara and the Hastings College of Law.

Welcome back, Jim.

Our final witness anchoring us today will be Mr. Edward Mierzwinski. Mr. Mierzwinski has served as consumer program director for the United States Public Interest Research Group, PIRG, a national and widely recognized consumer rights organization, since 1999.

He has testified before Congress and authored numerous advocacy reports on consumer issues relating to privacy, credit cards, credit reporting, and predatory lending practices. Mr. Mierzwinski is currently a member of the U.S.-European Consumer Coalition's Electronic Commerce and Privacy Working Group. He is a former

member of the Federal Resource Board of Governors' Consumer Advocacy Council, and served as executive director of Connecticut PIRG before joining the national organization. Mr. Mierzwinski is a graduate of the University of Connecticut.

We appreciate you bringing your considerable expertise to bear on this legislative effort today, Mr. Mierzwinski.

I would again like to thank all Members of this very distinguished panel for being here, and at this time we will turn to our first witness, Ms. Waters, for a 5-minute opening statement. And after each one of our witnesses has delivered their similarly limited 5-minute statement, we will turn to questions from the panel.

The record of these proceedings will remain open for 7 days so that any additional material that you all believe might be relevant or more lengthy statements can be submitted, and we would encourage all of the witnesses to keep that in mind so that we have as complete a record and as substantive a record to assist us in our deliberations and the deliberations of our colleagues as possible.

Ms. Waters.

**STATEMENT OF LORI L. WATERS, EXECUTIVE DIRECTOR,  
EAGLE FORUM**

Ms. WATERS. Thank you. I appreciate the invitation to be here this morning and discuss the issue of privacy and the impact that it has on Americans.

Technology has made it possible to store my life's entire records on a computer chip. Medical information, tax records, education records, Social Security contributions, et cetera, are all available to someone by merely a few key strokes on a computer. Controlling access to all my personal information is nearly impossible. Each classification of information has its own set of rules.

Privacy considerations are certainly not new. The fourth amendment is one of our most precious rights: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."

However, it is often the unintended consequences of laws that often have their most devastating impact on maintaining personal privacy. Social Security is a classic example. When Social Security was created in 1935, the sole purpose of the Social Security number was to track the earnings of employed Americans so that their wages could be properly credited. We were promised that the Social Security number would never be used for anything else, and so the first number was issued in 1936.

Well, where are we today? Social Security numbers appear on tax forms, medical records, some drivers' licenses, student I.D. cards, financial statements, marriage licenses, and even video rental applications. The Social Security number is the most used and abused number in America. A social insurance program for the elderly gave us each a Social Security number which today is used almost daily for non-Social Security purposes.

Now, let's turn to a more recent example of possible privacy implications of a recently enacted bill. On November 19, 2001, President Bush signed into law the Aviation and Transportation Security Act. The pertinent section reads as follows: Section 109. Enhanced Security Measures. In General—the Under Secretary of

Transportation for Security may take the following actions: Number (3) reads “Establish requirements to implement trusted passenger programs and use available technologies to expedite security screening of passengers who participate in such programs, thereby allowing security screening personnel to focus on those passengers who should be subject to more extensive screening.”

The privacy implications of this one section are overwhelming. Congress said that a trusted passenger program may be implemented, but neither the law nor report language established a single parameter for implementation. It will be up to the Under Secretary of Transportation for Security to answer the following questions in establishing trusted passenger requirements:

Who is a trusted passenger? Who will be eligible for the card? What information must the applicant give in order to verify who he says he is? Will the Government or private company maintain a database of trusted travelers? Will trusted passengers be tagged and tracked every time they use the cards? What will a trusted passenger card get you?

Well, further down in this same section of the Aviation and Transportation Security Act the Under Secretary of Transportation for Security may also “provide for the use of stress analysis, biometric, or other technologies to prevent a person who might pose a danger to air safety or security from boarding the aircraft of an air carrier or foreign air carrier in air transportation or intrastate air transportation.”

Again, there were no instructions on how to implement such a provision. In order to board a plane, will every passenger be forced to submit to a thumb print or retina scan? Who owns that information? An unelected official will likely end up answering every one of these questions.

Without proper consideration of privacy implications, the likelihood of a de facto national I.D. card is entirely possible. Members of Congress discuss it, but no one has taken ownership of the issue by introducing a bill entitled the National I.D. Card Act of 2002. Perhaps Members are smart enough to know that sponsorship of such a bill would be devastating to their reelection.

A national I.D. card or system could happen through the unintended consequences of regulations, merely connecting the dots of your life contained in the currently maintained Government and private databases. A trusted passenger program or national I.D. travel database could surge such a proposition forward.

In the name of security and anti-terrorism, proposals such as a national I.D. card, “know your customer” regulations, and Government databases to tag and track Americans are all on the discussion table, but bad ideas before 9/11 are still bad ideas today.

The need for the Federal Agency Protection of Privacy Act is clear. It is vital to protect Americans from unjustified and unintended invasions of privacy by the Government, and this bill would force regulators to consider how regulations impact personal privacy. And they must also tell citizens through a privacy analysis what that impact will actually be.

I appreciate the time this morning and look forward to your questions.

[The prepared statement of Ms. Waters follows:]

## PREPARED STATEMENT OF LORI L. WATERS

Technology has made it possible to store my life's entire records on a computer chip. Medical information, tax records, financial data, education records, Social Security contributions, driver records are all available to someone by merely a few key strokes on a computer. Controlling access to all of my personal information is nearly impossible. Each classification of information has its own set of rules.

Privacy considerations are certainly not new. The Fourth Amendment is one of our most precious constitutional rights: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."

However, it is often the unintended consequences of laws that have the most devastating impact on maintaining personal privacy. Social Security is a classic example. When Social Security was created in 1935, the sole purpose of the Social Security Number was to track the earnings of employed Americans so that their wages could be properly credited.

We were promised that the SSN would never be used for anything else, and the first number was issued in 1936. Social Security Numbers were clearly not created for identification purposes, and cards even stated that fact, well in the beginning. The temptation to use SSNs for other purposes was just too great. Today, they appear on tax forms, medical records, some driver's licenses, student ID cards, financial statements, marriage licenses, and even video rental applications. Today, SSNs are the most used and abused number in America. A social insurance program to care for the elderly gave each of us a Social Security Number, which today is used almost daily for non-Social Security purposes.

Let me give you one example of the possible privacy implications of a recently enacted bill. On November 19, 2001, President Bush signed into law the Aviation and Transportation Security Act (Public Law No: 107-71). The pertinent section reads as follows:

"Sec. 109. Enhanced Security Measures

- (a) IN GENERAL—The Under Secretary of Transportation for Security may take the following actions:
  - (3) Establish requirements to implement trusted passenger programs and use available technologies to expedite security screening of passengers who participate in such programs, thereby allowing security screening personnel to focus on those passengers who should be subject to more extensive screening."

The privacy implications of this one section are overwhelming. Congress said that a trusted passenger program "may" be implemented, but neither the law nor report language established a single perimeter for implementation. It will be up to the Under Secretary of Transportation for Security to answer the following questions in establishing trusted passenger requirements:

- 1) What is a trusted passenger?
- 2) Who will be eligible for a trusted passenger card?
- 3) How much information must an applicant give in order to verify who he says he is?
- 4) Will the government or a private company maintain a database of trusted travelers?
- 5) Will trusted passengers be tagged and tracked every time they use the cards?
- 6) What will a trusted passenger card get you?
- 7) To verify identity, will access to government databases be necessary or required? IRS? Social Security? New Hires Registry? Etc.

Further down in that same section of the Aviation and Transportation Security Act (Public Law No: 107-71), the Under Secretary of Transportation for Security may also:

- "(7) Provide for the use of voice stress analysis, biometric, or other technologies to prevent a person who might pose a danger to air safety or security from boarding the aircraft of an air carrier or foreign air carrier in air transportation or intrastate air transportation."

Again, there were no instructions on how to implement such a provision. In order to board a plane, will every passenger be forced to submit to a thumb-print or retina scan? Who owns that information? Will such information be kept on a database?

Will the government maintain the information on each airline? Or will the information merely be checked against a criminal or terrorist database?

An unelected official will end up answering all of these questions.

Without proper consideration of privacy implications, the likelihood of a de facto national identification card is entirely possible. Members of Congress discuss it, but no one has taken ownership of the issue by introducing a bill entitled: the National ID Card Act of 2002. Members are smart enough to know that sponsorship of such a bill would likely be devastating to their re-election. A national ID card or system could happen through the unintended consequences of regulations, merely connecting the dots of your life contained in the currently maintained government and private databases. A trusted passenger program or national travel database could surge such a proposition forward.

In the name of security and "anti-terrorism," proposals such as a National I.D. card, Know-Your-Customer banking systems, and expansion of government databases to tag and track Americans are all on the table for discussion. Bad ideas before 9/11 are still bad ideas now.

Back to the Fourth Amendment, most lawyers have argued over the definition of unreasonable, so I will not. However, I will say that it is unreasonable to morph America into a place where everyone is treated as a terrorist, deadbeat dad, money launderer, drug trafficker, or criminal. Tagging and tracking the everyday actions of law-abiding citizens is inconsistent with freedom, liberty, and American values. Only totalitarian regimes monitor the private actions of law-abiding citizens.

The need for the Federal Agency Protection of Privacy Act (H.R. 4561) is clear. It is vital to protect Americans from unjustified or unintended invasions of privacy by the government. H.R. 4561 forces regulators to consider how regulations impact on individual privacy and then they must tell citizens through a privacy analysis what the impact will actually be.

Long-term privacy consequences must be part of the legislative debate in Congress as well as the regulatory debate in the Executive Branch. Government agencies are often awarded the great task of working out the details when it comes to privacy. For instance, the 1996 Health Insurance Portability and Accountability Act gave the Department of Health and Human Services the power to draft medical privacy regulations if Congress did not act by August 21, 1999. Well, HHS is still working on final (watered-down) regulations. Privacy was clearly at the center of these regulations, but while implementing other laws, like Social Security or trusted passenger, privacy implications should also be considered.

The Federal Agency Protection of Privacy Act is a positive step to assessing privacy implications inflicted by the government, but Congress should not stop there. Greater protections are necessary in order to regain control of our personal information.

As the government collects personal information, its use should be restricted to the purpose for which it was originally demanded and received. The government should not be able to act as though it owned that information to sell, display, or traffic without our consent.

Congress should not only look at the massive intricacies of privacy-invasive laws already on the books (and repeal a few) but should also look forward to what is coming.

Technology is developing more rapidly than any of us can follow, but the law often lags behind. Are you ready for the implantable chip? Applied Digital Solutions, a company traded on the NASDAQ, has developed implantable microchips for humans, and people are already signing up. The Food and Drug Administration said in April 2002 that it would not regulate the use of implantable microchips for ID purposes as long as it contains no medical information. ADS's Verichip will contain a scanable ID number that could then be cross-referenced with any number of databases.<sup>1</sup> "Big Brother" lives.

Is the law ready for such privacy-sensitive technology? It's up to you as Members of Congress to make sure it is.

Mr. BARR. Thank you very much, Ms. Waters. And, again, if there were portions of your opening statement that you didn't have time to read and would like those a part of the record, they will be made a part of the record.

Ms. WATERS. Thank you.

Mr. BARR. Thank you.

<sup>1</sup>"ID chip ready for implant," April 4, 2002, *USA Today*.



Mr. Nojeim.

**STATEMENT OF GREGORY T. NOJEIM, ASSOCIATE DIRECTOR  
AND CHIEF LEGISLATION COUNSEL, AMERICAN CIVIL LIB-  
ERTIES UNION**

Mr. NOJEIM. Chairman Barr, Ranking Member Watt, Members of the Subcommittee, I am pleased to testify today in favor of the Federal Agency Privacy Protection Act on behalf of the ACLU. Ours is a nationwide non-profit organization with nearly 300,000 members dedicated to protecting the principles of freedom set forth in the Constitution and our Nation's civil rights laws. We join many Members of this Subcommittee on both sides of the aisle, and non-governmental organizations from across the political spectrum, in support of this legislation.

Americans' right to privacy is in peril. Individuals' personal information, including medical and financial records, is being collected on computer networks that can be linked, transferred, shared, and sold, often without consent or knowledge of the person to whom it pertains.

In this context, where personal information is maintained by the Government, the fourth amendment is little help. That is because the courts have held in many cases that the fourth amendment doesn't apply when the information is held by a third party. If it is not in your desk drawer, it is already held by the Government. In situations like this, legislation is essential to protect privacy.

The legislation that you are considering is simple yet powerful, and modest yet effective.

It would require Federal agencies to issue privacy impact statements with the regulations they propose. It would encourage agencies to develop a systematic means for reviewing how a particular regulation would affect privacy.

Apply these principles to the trusted passenger program that Ms. Waters just described. It would mean that the Transportation Security Agency would have to consider what data it would gather about the passengers who might be given these cards and whether it could collect less data and achieve the same security outcome that it could get by collecting more data.

This bill introduces long-accepted principles of fair information practices into the rulemaking process. It is modeled after the Regulatory Flexibility Act and it places an important check on agencies' use and disclosure of personal information.

People care about privacy. Under this bill, they will have a better opportunity to be heard when their privacy is threatened.

I called the bill "modest" because what it does not do is as important as what it does do. The bill does not create new, substantive legal standards for the use and disclosure of individually-identifiable personal information maintained by Government agencies. The Privacy Act and other Federal statutes already do this.

The bill does not give an individual the power to force an agency to adopt a particular policy alternative, including the alternative least intrusive of privacy. It merely requires agencies to consider less intrusive alternatives and to explain why they selected one alternative over the others.

The bill is not overly burdensome and it would not hinder the efficient functioning of Federal agencies. The legislation applies only to rulemaking. It does not cover other more numerous administrative actions that fall outside the formal rulemaking process. These are things like adjudications and informal agency actions. In particular, law enforcement agencies would continue to be able to investigate crimes and track down criminals just as they do under current law.

The bill includes necessary exceptions from its requirement for privacy impact statements, and it incorporates other exceptions that already appear in current law. Many agency actions are already exempt from the rulemaking process. For example, if rulemaking procedures are impracticable, unnecessary, or contrary to the public interest, no rule must be proposed at all. In such circumstances, the Federal Agency Privacy Protection Act would not require a privacy impact statement. In fact, under this legislation privacy impact statements would not even be required in a formal rulemaking when an emergency makes compliance impracticable.

The bill would not spawn overwhelming litigation. The judicial review this legislation authorizes is limited to review of agency compliance with procedures related to the final privacy impact statement. It does not provide individuals a right to sue over the substantive decisions the agency makes in the final regulation.

I want to be clear here. An agency's determination to adopt a regulation invasive of privacy is not in and of itself a ground for a lawsuit under the act. Failure to consider the alternatives is, and should be.

Mr. Gekas, we agree that judicial review is crucial to ensure agency compliance with the very limited procedures that this bill would require.

Mr. Barr, you have brought forward this legislation at an important time in American history. Since the terrible events of September 11, Congress and the Administration have considered numerous proposals that would undermine privacy in the name of security. Your legislation would require agencies to consider both safety and privacy as they develop new regulatory schemes. We urge you to move it to the House floor expeditiously.

Thank you.

[The prepared statement of Mr. Nojeim follows:]

PREPARED STATEMENT OF GREGORY T. NOJEIM AND KATIE CORRIGAN

The American Civil Liberties Union is a nationwide, non-partisan organization of nearly 300,000 members dedicated to protecting the principles of liberty, freedom, and equality set forth in the Bill of Rights to the United States Constitution. For almost 80 years, the ACLU has sought to preserve and strengthen privacy in many aspects of American life.

Americans' right to privacy is in peril. Individuals' personal information, including medical and financial records, is being collected through an ever expanding number of computer networks and being stored in formats that allow the data to be linked, transferred, shared and sold, often without consent or knowledge.

The same technological advances that have brought this country enormous benefit also make people more vulnerable to unwanted snooping and accidental disclosure of personal information. The federal government's increased reliance on computerized records increases efficiency but also poses significant challenges to privacy.

H.R. 4561, the "Federal Agency Protection of Privacy Act," would require federal agencies to issue privacy impact statements with the rules or regulations they propose. By requiring privacy impact statements, the bill would encourage agencies to

develop a systematic means for reviewing how a particular regulation would affect individual privacy. In addition, such statements would put the public on notice about the choices federal agencies are making about the use and disclosure of individually identifiable information and give the public a carefully limited chance to participate in those decisions.

The Federal Agency Protection of Privacy Act would provide an important check and balance on federal agencies' use and disclosure of personal information inside and outside the government. The passage of this legislation would be an important step in the effort to protect privacy, particularly as the federal government relies more and more on powerful information technology.

#### THE HISTORY AND LESSONS OF THE "KNOW YOUR CUSTOMER" BANKING REGULATION

The history of the "Know Your Customer" ("KYC") regulations provides important background on the need for privacy issues to be considered before a regulation is adopted.

In 1998, pursuant to the Bank Secrecy Act and other federal law, each of the bank regulatory agencies published parallel "Know Your Customer" regulations to facilitate the filing of suspicious activity reports, an element of the agency's broader anti-money laundering initiative. Most banking institutions already had adopted KYC programs voluntarily. The proposed regulations, however, would have mandated uniform standards across the banking industry.

The purpose of the KYC regulations was to facilitate the financial institution's compliance with anti-money laundering laws and to protect the financial institution from accidentally facilitating criminal activity. The proposed rule required banks to establish uniform systems to identify customers and their normal and expected transactions, to determine the customer's sources of funds for transactions involving the bank, and to monitor daily transactions and identify those that appear suspicious.

The impact of the regulation, however, would have been to require banks to track innocent individuals in their day to day financial transactions and collect and track an enormous amount of personal financial information through federal databases. The Comptroller of Currency made a nod to privacy in the preamble of its proposed KYC regulations by requiring a bank to "obtain only that information that is necessary to comply with the regulation and . . . limit the use of this information to complying with that regulation." Generally, however, the agencies were taken by surprise when an avalanche of public criticism came down on the proposed KYC requirements.

In 1999, the Treasury Department was overwhelmed by almost 300,000 comments on "Know Your Customer" regulations because the agency failed to consider the privacy implications of tracking customers' routine banking activities and reporting personal financial information to the government before issuing the rule. As a result, the agency was forced to retreat and withdraw the rule.

The KYC experience provides two clear lessons. First, Americans care about the privacy of personal information. Out of the almost 300,000 comments submitted on the proposed KYC regulations, only a small fraction were in favor of the regulation. Second, federal agencies must consider privacy up front. As demonstrated by the proposed KYC regulations, because bank regulators failed to consider privacy, the proposed regulation unraveled, forcing regulators back to the drawing board and wasting federal resources.

#### REQUIREMENTS OF THE FEDERAL AGENCY PROTECTION OF PRIVACY ACT

Although there are federal laws regulating the use and disclosure of personal information within the government, privacy continues to be an afterthought in the development of federal policy. In addition, the public has little opportunity to comment on—or even understand—the choices administrators are making about the use and disclosure of individually identifiable information.

The Federal Agency Protection of Privacy Act would establish basic checks and balances on federal agencies' decisions to use and disclose personal information. The legislation's "privacy impact statement" builds the principles of Fair Information Practices into the rulemaking process and would enhance individuals' control over personal information stored in government databases.

The bill would require agencies to engage in a systematic review of privacy before federal regulations are adopted and irreversible privacy violations occur. In addition, it would enhance federal agencies' public accountability for decisions about the use and disclosure of personal information.

This legislation is modeled after the Regulatory Flexibility Act ("RFA"). 5 U.S.C. §601 seq. For over twenty years, it has required agencies to consider the needs and

concerns of small business whenever they engage in rulemaking subject to the notice and comment requirements of the Administrative Procedure Act (“APA”) or other federal law. This bill adopts requirements almost identical to those found in the RFA. Instead of assessing the impact on small business, however, the agency analyses would assess the impact of a regulation on individual privacy.

#### WHAT THE BILL WOULD DO:

*Require a systematic review of privacy issues before a regulation is adopted.*

Sections 2(a) and (b) would require federal agencies to issue initial and final privacy impact analyses whenever the agency is required under the APA or other federal law to publish a general notice of proposed rulemaking, including interpretative rules involving tax laws.

The “initial privacy impact analysis” would be published with the agency’s proposed rulemaking and the public would have an opportunity to comment on the privacy impact statement and the underlying regulation. The contents of the impact analysis would include an assessment of the extent to which the proposed rule will impact individual privacy interests including: 1) what personally identifiable information is to be collected, and how it is to be collected, maintained and used; 2) whether and how individuals can access the personal information that pertains to them; 3) how the agency prevents the information collected one purpose from being used for another purpose; and 4) what security safeguards are in place to prevent unauthorized disclosure of personal information. Most importantly, the agency must describe alternatives to the proposed rule which accomplish the policy objective but minimize impact on individual privacy.

A “final privacy impact analysis” would be issued with the final rule or regulation. This final privacy impact statement would include the same categories of information as the initial impact statement. In addition, the agency would have to explain the steps it has taken to minimize the “significant” privacy impact on individuals, including the factual, policy and legal reasons for selecting the alternative adopted in the final rule and why the other alternatives were rejected. The final privacy impact statement would also summarize the significant issues raised in the public comments.

*Enhance public participation and agency accountability for individual privacy interests.*

Section 2(d) would require the federal agency proposing a rulemaking that would have a “significant privacy impact on individuals, or a privacy impact on a substantial number of individuals” to ensure individuals have been given an opportunity to participate. It could do this by taking steps such as announcing the rulemaking’s potential privacy impact in publications with a national circulation, holding public hearings and conferences, and directly notifying interested individuals.

Section 2(f) would provide individuals who are “adversely affected or aggrieved” by final agency action to obtain judicial review of compliance with the procedures for final privacy impact statements.

Section 2(e) would require a periodic review of rules that have a “significant privacy impact on individuals, or a privacy impact on a substantial number of individuals” to determine whether a rule can be amended or rescinded to minimize an adverse privacy impact. Such review is required to take place within ten years of the date of enactment of the regulation. Agencies are also required to publish plans for these reviews in the Federal Register and invite public comment on whether the rule should be rescinded or amended.

#### WHAT THE BILL WOULD NOT DO:

The Federal Agency Protection of Privacy Act would take important steps to protect privacy. Equally important, however, the legislation would not undermine government rulemaking process or inhibit important government policy goals.

First, the bill does not create new substantive legal standards for the use and disclosure of individually identifiable personal information within the federal government. The Privacy Act and other federal statutes continue to regulate the use and disclosure of personal information held by federal agencies. Sections 2(a) and (b) simply offer criteria that would be used to measure the privacy impact of any particular regulation.

Second, the bill does not give an individual the power to force an agency to adopt a particular policy alternative. The final privacy impact analysis requires agencies to articulate the available policy options and state why one alternative was selected over the others. But, the bill does not require the agency to adopt the alternative that is least intrusive on privacy.

Third, the bill is not overly burdensome and would not hinder the efficiency or functioning of federal agencies. The legislation only applies to rulemaking, not to the vast amount of administrative action that falls outside the formal rulemaking process, including adjudication, informal action, and guidance.<sup>1</sup> Law enforcement agencies would continue to be able to investigate crimes and track down criminals just as they do under current law. In addition, a privacy impact analysis would only be required if a rulemaking is required in the first place. The APA includes exceptions that exempt certain agency functions from the rulemaking process altogether, including when rulemaking procedures are “impracticable, unnecessary, or contrary to the public interest.” In addition, privacy impact statements could actually increase efficiency by cutting down on privacy debacles like the proposed KYC regulation. Lots of government resources were wasted on that proposed rule because there was little to no consideration of privacy in the development of the proposed regulations.

Fourth, the bill would not result in an overwhelming amount of litigation. Judicial review is limited to review of agency compliance with the procedures related to the final privacy impact statement. It does not provide individuals a right to sue over substantive decisions the agency makes in the final regulation. In 1996, the Small Business Regulatory Enforcement Fairness Act established the same judicial review provisions in the RFA as are included in this legislation. Pub.L. 104–121.

Finally, the legislation includes the same waivers available under the RFA. Privacy impact statements would not be required when emergencies make compliance “impracticable.”

#### CHALLENGES TO PRIVACY ON THE HORIZON

The Federal Agency Protection of Privacy Act is considered at an important time in American history. Since the terrible events of September 11, numerous proposals have been introduced in the Congress and proposed by the Administration that would undermine civil liberties in the name of security.<sup>2</sup> Americans remain concerned about privacy, however.<sup>3</sup>

This legislation would require agencies to consider both safety and privacy as they implement regulations on a range of security measures. Specifically, the legislation’s privacy impact assessments would require agencies to identify policy alternatives that would achieve the same security goal while limiting the impact on privacy.

The legislation would have an important impact on several security proposals the Administration is currently considering. For example:

*National ID proposals:* Last fall’s air security legislation requires the new Transportation Security Administration to consider implementation of a trusted passenger program. P.L. 107–71. The text of the legislation fails to detail the elements of the program, but its purpose would be to expedite security screening by establishing the identity of “trusted” passengers through the issuance of an ID card. The trusted passenger program is a tempting measure because it would provide frequent travelers a convenient route through the airport. Trusted passengers, however, cannot be trusted. “Sleeper cell” terrorists could easily be among the trusted passengers and thereby avoid heightened screening measures.<sup>4</sup>

<sup>1</sup>In comparison, the Canadian government announced its own “Privacy Impact Assessment Policy” last week. The Canadian requirements apply to “any program or service delivery initiatives” at government institutions. Privacy Impact Assessment Policy, effective date May 2, 2002. <http://www.tbs-sct.gc.ca/pubs-pol/ciopubs/pia-pefr/paip-pefr-e.html>.

<sup>2</sup>See e.g. Uniting and Strengthening America By Providing Appropriate Tools Required To Intercept and Obstruct Terrorism Act (“USA PATRIOT Act”). Pub. L. No. 107–56 (2001).

<sup>3</sup>This concern is reflected by the public’s dwindling interest in national ID systems. “Immediately after the attacks, a Harris Poll found that 68% of Americans supported a national ID system. A study conducted in November 2001 for the Washington Post found that only 44% of Americans supported national ID. A poll released in March 2002 by the Gartner Group found that 26% of Americans favored a national ID, and that 41% opposed the idea.” <http://www.epic.org/privacy/survey/default.html>

<sup>4</sup>On February 5, 2002, Under Secretary John Magaw was asked about the trusted passenger card during a Senate Commerce Committee hearing on air security. Magaw said he would be hesitant to allow any passenger to avoid passenger and baggage screening requirements. “[M]y whole problem is that this may be . . . not as good as it looks to be. It may be convenient, but in terms of security, I don’t really see it helping us, because I would not be willing to . . . allow the baggage to go unchecked or have your hand carry unchecked. So I don’t really see the benefit of it in terms of security.”

Such a system also cuts to the heart of privacy and freedom because it is a de facto national ID.<sup>5</sup> The card would link a multitude of databases containing personal information through unique identifiers for each air traveler.

The Administration should reject this measure entirely. At a minimum, however, there should be some consideration of other policy options that would achieve the same level of security benefit, without establishing a national ID. The Federal Agency Protection of Privacy Act would require the TSA to do just that.

*Financial Privacy:* Title III of the USA PATRIOT Act continued the unfortunate trend of expanding government access to personal financial information rather than safeguarding it against intrusion. P.L. 107–56. The Treasury Department has issued nine sets of regulations in the last six months to comply with Title III's anti-money laundering requirements. Just last week, the Treasury Department issued regulations that apply anti-money laundering rules to mutual funds, credit card systems, money transfer companies and check cashers, and securities and commodities brokers in addition to the banking industry.

And, the Treasury Department's work is not complete. The agency is currently working on anti-money laundering regulations that will apply to a range of other industries including dealers in precious metals and jewels, pawnbrokers, loan or finance companies, private bankers, insurance companies, travel agencies, telegraph companies, real estate brokers.<sup>6</sup>

While there is a need to shut down the financial resources used to further acts of terrorism, the expansion of anti-money laundering programs, including suspicious activity reporting, reaches into innocent customers' personal financial transactions. In addition, it is unclear that if the government collects more and more information about individuals' financial transactions law enforcement agencies will in fact be able to identify terrorist activity. There are millions of innocent financial transactions every year.<sup>7</sup>

H.R. 4561 would require agencies to consider the privacy implications of collection, use and disclosure of massive amounts of individually identifiable financial data reported in suspicious activity reports from all of these industries and the exchange of such information between federal agencies and private industry.

The legislation would not require the agency to choose a particular policy alternative, but it would force the agency to articulate what steps have been taken to minimize the privacy impact of the regulation and identify the policy alternatives that were rejected.

In addition, Section 2(d) of the bill would require a review of these regulations within ten years to determine if the rule could be modified or rescinded entirely to minimize the impact on privacy. These regulations clearly have a privacy impact on a "substantial number of individuals."

As new security measures are introduced, the Federal Agency Protection of Privacy Act ensures that agency will ask questions about privacy up front, before a regulation is adopted.

#### CONCLUSION

The ACLU strongly commends the Chairman Barr (R-GA) and Congressmen Watt (D-NC), Gekas (R-PA), Nadler(D-NY), Chabot (R-OH), and Green (R-WI) for introducing this important bill. We urge other Members to join them in support of a good government measure that would enhance individuals' privacy.

Mr. BARR. Thank you very much, Mr. Nojeim, and I know from looking at your written statement there are a lot of specific items that you left out in the interest of getting through those. And I hope we have a chance to maybe touch on a couple of them during the Q and A, but they will be made a part of the record.

Thank you.

Mr. Harper, please.

<sup>5</sup> National Research Council, *IDs—Not That Easy: Questions About Nationwide Identity Systems*, (Stephen T. Kent and Lynette I. Millett eds., 2002).

<sup>6</sup> 31 C.F.R. Part 103, Financial Crimes Enforcement Network, Anti-Money Laundering Programs for Financial Institutions, Interim Final Rule, April 23, 2002.

<sup>7</sup> See Veronique de Rugy, Sam Spys: *The Case Against Watching Everyone*, NATIONAL REVIEW ONLINE, Dec. 17, 2001. ("Part of the problem is that money-laundering laws create an ocean of data that law enforcement cannot hope to navigate.")

**STATEMENT OF JAMES HARPER, EDITOR, PRIVACILLA.ORG,  
AND ADJUNCT FELLOW, PROGRESS AND FREEDOM FOUNDATION**

Mr. HARPER. Thank you, Mr. Chairman, Mr. Watt, Members of the Subcommittee, including my old Chairman, Mr. Gekas. It is a pleasure to be before you today to discuss the——

Mr. BARR. You described him as “old?” [Laughter]

Mr. HARPER. Past Chairman.

Mr. BARR. Thank you.

Mr. HARPER. It is a pleasure to discuss the Federal Agency Protection of Privacy Act. I am Jim Harper, the Editor of Privacilla.org, a Web-based think tank devoted exclusively to the subject of privacy as a public policy issue.

Privacilla attempts to capture privacy as a public policy issue from top to bottom. We deal with privacy from Government, privacy in the private sector, including financial, medical online, and fundamental privacy concepts. I have placed a copy of my written statement on the site with annotations and links that readers can use to reach more information about the material I have submitted to you.

Privacilla does take a free-market, pro-technology view of privacy policy. There are other views, and I urge you to consider them all. Many of them are represented here at the table today. Please also know that Privacilla is a project of my consulting firm, PolicyCounsel.com, not separately incorporated. My firm does not represent anyone on privacy specifically, but privacy touches nearly every public policy issue. So be aware of my potential for bias as you consider my testimony. The views I am expressing today are my own and not those of any client.

Chairman Barr, congratulations to you for introducing H.R. 4561 with the broadly bipartisan support that you have gotten. Mr. Watt and other Members of the Subcommittee, congratulations to all of you for being original cosponsors.

I have a lot to say about this legislation in terms of privacy, but let me reach back into some of my work on administrative law and discuss the administrative law aspects at the outset.

There is ample precedent for the changes to the Administrative Procedure Act that would be mean by the Federal Agency Protection of Privacy Act. As Mr. Nojeim mentioned, the Regulatory Flexibility Act, originally passed in 1980, is the model for this legislation.

Each time an agency publishes a proposed rule in the Federal Register, it must issue an initial regulatory flexibility analysis that examines and describes the impact of the rule on small entities like small businesses, small organizations, and small governments.

The initial reg flex analysis is subject to public comment, and a final regulation must be accompanied by a final regulatory flexibility analysis that, based on those comments and other analysis, discusses again the impact of the rule on these small entities. This is the successful model that is used for the Federal Agency Protection of Privacy Act we are discussing today.

Along similar lines, Congress passed the Unfunded Mandates Reform Act in 1995 and the Small Business Regulatory Enforcement Fairness Act in 1996 to require agencies to work more closely with

local governments and small businesses in formulating regulations. It also subjected, as you mentioned, Mr. Gekas, the analysis requirements of the Reg Flex Act to judicial review.

Obviously, since the Federal administrative process has been modified over the past 25 years to consider the interests of small business, small governments, it is about time that the Federal administrative process be modified to consider the interests of Americans in maintaining privacy.

Though Government programs are motivated by only the best intentions, many of them deprive Americans of control over information about themselves. The Federal Agency Protection of Privacy Act can help restore to people their power over personal information.

When citizens apply for licenses or permits, fill out forms for regulators, or submit tax returns, they do not have the legal power to control what information they will share. It is either illegal to withhold information or the penalty for withholding information is deprivation of money or benefits to which citizens are legally entitled.

It will be a mammoth but worthwhile task to reorient the regulatory process toward consideration of privacy. The bureaucracy will not regard this as a walk in the park, and I would not expect them to volunteer their support of this legislation. But nearly every Federal agency has one or more databases of personal information, sometimes very sensitive, private medical and financial information, and they are not afraid to use this information.

In March 2001, Privacilla issued a report finding that Federal agencies begin a new program to merge databases more than once every 2 weeks. These programs are only the tip of an information-trading iceberg. The Privacy Act requires only notice of a new routine use in the Federal Register before personal data is used and shared in new ways.

In case it needs emphasis again, the political leaders who create such programs and the administrators who operate them have the best of intentions for serving the public. Similarly, the fact alone that a program weakens Americans' privacy should not be the sole reason to terminate or reduce a program. Rather, privacy should be an important factor that policymakers consider whenever they are creating, implementing, or altering Government programs. The Federal Agency Protection of Privacy Act will make consideration of privacy part of the policymaking calculus in Federal agencies and in the Congress.

There is a great deal more material in my written statement that I encourage you to review. In particular, I draw your attention to the definition I have offered for the term "privacy" and to my discussion of the so-called fair information practices. There is plenty of room to quibble about the fair information practices among people who all are expressing support for the bill today. Many different and sometimes competing policies are found in this area.

As you consider this legislation, keep clearly in mind the various information policies that are sometimes too easily lumped together. Though it may sound trite, information is power, and increasingly so in our technological present and future. Governments alone, as you observed, Chairman Barr, can take information from people by force of law.



We have many reasons, I think, to be proud of the restraint that our Government shows, but particularly with the growth of databases and communications technologies, we have many reasons to be cautious, too. The notorious "Big Brother" in George Orwell's "1984" was written as a caution against the power of governments. In some circles, there is talk of a coming privacy Exxon Valdez, and I believe that if a privacy disaster is to come, I am nearly certain it will be a Government database that runs up against the rocks. The Federal Agency Protection of Privacy Act may help steer the ship away from the shoals and give people back some power over information.

Thank you.

[The prepared statement of Mr. Harper follows:]

#### PREPARED STATEMENT OF JIM HARPER

Chairman Barr, Mr. Watt, and Members of the Subcommittee:

It is a great pleasure to appear before you to discuss H.R. 4561, the "Federal Agency Protection of Privacy Act." I am Jim Harper, the Editor of Privacilla.org, a Web-based think-tank devoted exclusively to privacy. I am also an Adjunct Fellow at the Progress & Freedom Foundation and the Founder and Principal of Information Age lobbying and consulting firm PolicyCounsel.Com.

Privacy is one of the most complex and difficult public policy issues confronting Congress and legislatures across the country today. I am pleased to lend what knowledge I have to your consideration of this legislation.

Privacilla.org is a Web site that attempts to capture "privacy" as a public policy issue. The pages of Privacilla cover the issue of privacy from top to bottom. We deal with fundamental privacy concepts, privacy from government, and privacy in the private sector, including financial, medical, and online privacy. Anyone may submit ideas, information, and links for potential inclusion on the site. The site represents the thinking of many people and I would refer you to the Privacilla "Support" page to get an idea of the groups we work with. Please visit Privacilla at <http://www.privacilla.org> and use it as a resource whenever your work brings you to a privacy policy question.

Privacilla takes a free-market, pro-technology approach to privacy policy. There certainly are other views, and you should consider them all. Please also be aware that Privacilla is currently a project of my lobbying and consulting firm, PolicyCounsel.Com. My firm does not represent any interest on privacy specifically, but nearly all issues touch on privacy in some way, so you should consider my potential for bias, as you would with any privacy advocate. The views presented on Privacilla, and those I express today, are not the views of any client.

Chairman Barr, I salute you for introducing H.R. 4561 with broadly bipartisan support, and for holding these hearings today. Mr. Watt, and other Members of the Subcommittee, congratulations to you for joining in introducing this important bill.

Privacy is a complex and widely misunderstood public policy issue. This legislation can help protect Americans' privacy by giving the American people, the press, and Congress information they need about how federal regulation affects privacy. This legislation presents an opportunity to refine the terms of the many different "privacy" debates, so that Congress, the press, and the public can find solutions to a number of important problems.

Though they are motivated only by beneficent purposes, many government programs deprive Americans of control over personal information and their privacy. The Federal Agency Protection of Privacy Act can help restore to the people the power and autonomy that is one of the great benefits of living in the United States. There are several successful precedents in our nation's administrative laws for this proposal. Few, if any, changes are needed to perfect the legislation in terms of privacy. I urge you, though, to be aware of the many important elements of information policy beyond privacy that fall within the scope of the bill.

#### DEFINING TERMS: WHAT IS PRIVACY?

The Judiciary Committee is the committee of American law and legal institutions. There is no better place to define and give structure to terms such as our focus today: privacy. By digging deeply into privacy as a legal concept, you as congressional leaders can dramatically improve the quality of many public policy debates, and the outcomes Congress produces for the American people.

Left undefined, the word “privacy” has become far too much of a stalking horse for all variety of ideological and special interest groups. Indeed, a coterie of activist organizations—including Privacilla—thrives because there is not an agreed to and limited definition for the word “privacy” in current debate. Moreover, the lack of definition has rendered Congress, state legislatures, the press, and the public less able to find solutions to the many problems and legitimate concerns that popularly fall under the heading of “privacy.”

For example, identity fraud is widely perceived as a “privacy” problem. But it is better understood as a group of crimes that thrive on the use of personal identification and financial information. Because of this widespread misperception, the crimes that constitute identity fraud go poorly enforced while Congress considers banning many uses of Social Security Numbers in the name of “privacy.” Limiting SSN use would likely stifle many benefits that consumers and the economy enjoy without effectively reducing this serious crime problem.

Similarly, unwanted commercial e-mail, or “spam,” is an intrusion into electronic communications and a serious annoyance that is often labeled as a “privacy” problem. Spam exists in large part because e-mail marketers know little or nothing about the interests of potential customers. It is difficult to reconcile spam—e-mails broadcast to unknown people nearly at random—with the heart of the privacy concept, which is too much personal information being available too widely.

At Privacilla, we have a working definition of privacy that we believe should form the basis of policy discussions on the topic: *Privacy is a subjective condition that individuals enjoy when two factors are in place—legal ability to control information about oneself, and exercise of that control consistent with one’s interests and values.*

Privacy is a personal, subjective condition. It is a state of affairs individuals enjoy based on sharing or retention of information about themselves consistent with their own preferences. These preferences are a product of such things as culture, upbringing, and experience. Because privacy is subjective, one person cannot decide for another what his or her sense of privacy should be. You can not tell me, either by giving your opinion or by passing a law, that my privacy is protected when I think it is not.

The first factor above goes to the existence of choice—the legal power to control the release of information. A person who wishes to maintain privacy in the appearance of his or her body, for example, may put on clothes and be relatively certain that no one will remove that clothing without permission. Few laws require people to remove their clothing and, thanks to the concept of “battery” in state tort and criminal law, private actors may be punished for touching our clothing in any way that interferes with bodily privacy. Our choices to hide or reveal information about the appearance of our bodies are protected by law.

Likewise, a person who wants to prevent others from gaining knowledge of his or her purchasing patterns may pay in cash and regularly change the stores at which he or she shops. He or she may also arrange by contract to have personal information maintained in confidence. Various legal protections, such as the law of contracts, give us autonomy and choice that we use to protect privacy.

The second factor is exercising that control of information consistent with our values. This is difficult in many commercial marketplaces. Many consumers are unaware of how the Information Economy works, and the fact that they are a part of it. Many industries are monolithic in their information practices. Arguably, they fail to fully inform consumers about what happens with personal information, and they offer consumers few alternatives. This is arguable, however. It may be that only a tiny, but vocal minority of consumers and activists actually wants to study commercial information practices and exercise choice among different options. If a significant number of consumers do, they are a market waiting to be served.<sup>1</sup>

As policy-makers, we should not presuppose that a certain amount or type of privacy serves consumers’ interests in the marketplace, and Privacilla’s definition of privacy does not do this. Advocates who claim to know what consumers want in terms of privacy prove their ignorance by making the claim.

Consumers may rationally determine that they are safe from harmful uses of information when dealing with certain companies and leave it at that. The fact that hundreds or even thousands of mundane facts about themselves are in the hands of businesses may be a matter of indifference to reasonable people. Aware, empowered, and responsible consumers can demand of businesses what options they want in terms of information sharing or withholding. They can also demand, if they prefer, lower prices, customized service, combined offerings, and so on.

<sup>1</sup> See Paul H. Rubin and Thomas M. Lenard, *Privacy and the Commercial Use of Personal Information*, Progress & Freedom Foundation (July 2001) <<http://www.pff.org/RubinLenard.pdf>>.

Unless Congress and state legislators are going to guess at consumers' true preferences and impose them from the top down, only consumer education will deliver privacy on the terms consumers want it in the commercial world. Governments cannot protect privacy directly; they can only foster or destroy people's ability to protect their own privacy.

#### GOVERNMENTS POSE A UNIQUE THREAT TO PRIVACY

While protecting privacy in the commercial world may be difficult, protecting privacy from government is impossible. Dealings with government are categorically different from interactions in the private sector. When citizens apply for licenses or permits, fill out forms for regulators, or submit tax returns, they do not have the legal power to control what information they share. They must submit the information that the government requires. It is either illegal to withhold information or withholding information penalizes citizens of money or benefits to which they are legally entitled. The notorious "Big Brother" in George Orwell's *1984* was a caution against the powers of governments. When dealing with them, the first factor in privacy protection—legal power to control personal information—is absent.

It would be a mammoth, but worthwhile, task to catalogue all the personal information that is demanded by all federal programs. Additional study should include the purposes for which information is collected, other purposes to which it is put, and whether such information is ever eliminated from government records when it has served its original or successor purposes. The Federal Agency Protection of Privacy Act may help us do that.

Some studies suggest the scope of personal data collection and warehousing done at the federal level. In September 2000 testimony to the House Government Reform Subcommittee on Information Management, Information, and Technology, Solveig Singleton, now of the Competitive Enterprise Institute, surveyed federal databases.<sup>2</sup> Her non-exhaustive list included databases at the Commerce Department, the Department of Justice, the Department of Education, the Department of Energy, the Federal Bureau of Investigation, the Department of Health and Human Services, the Department of Housing and Urban Development, the Department of the Interior, the Department of Labor, the Social Security Administration, and the Department of the Treasury, which houses the Internal Revenue Service. Many of these databases include health and financial information.

In March 2001, a study issued by Privacilla.org found that, during the 18-month period from September 1999 to February 2001, federal agencies announced 47 times that they would exchange and merge personal information from databases about American citizens. New information sharing programs were instituted more than once every two weeks.<sup>3</sup> We characterized these programs as only the tip of an information-trading iceberg. The Computer Matching and Privacy Protection Act,<sup>4</sup> which causes agencies to report these activities in the Federal Register, applies only to a small subset of the federal agency programs that use personal data about Americans. New uses of personal information are made by federal agencies constantly. The Privacy Act requires only a declaration in the Federal Register of a new "routine use" before personal data is used and shared in new ways.<sup>5</sup>

In case it needs emphasis, the threats to privacy posed by government programs are not the result of malice or malfeasance of any kind. The political leaders who have instituted such programs, and the administrators who operate them, have the best intentions for serving the public. Similarly, the fact alone that any government program weakens American citizens' privacy should not be the sole reason to terminate or cut back the program. Rather, privacy should be an important factor that policy-makers consider whenever they are creating, implementing, or altering government programs. Studies like *Privacy and the Digital State: Balancing Public Information and Personal Privacy* by Progress & Freedom Foundation Senior Fellow Alan Charles Raul have made progress on that front. The Federal Agency Protection of Privacy Act would help make privacy part of the policy-making calculus in federal agencies and in the Congress.

<sup>2</sup> Solveig Singleton, *Testimony Before a Hearing of the Subcommittee on Government Management, Information, and Technology on "Computer Security: How Vulnerable Are Federal Computers?"*, September 11, 2000 <<http://www.house.gov/reform/gmit/hearings/2000hearings/000911computersecurity/000911ss.htm>>.

<sup>3</sup> Privacilla.org, *Privacy and Federal Agencies: Government Exchange and Merger of Citizens' Personal Information is Systematic and Routine*, March 2001 <<http://www.privacilla.org/releases/Government-Data-Merger.html>>.

<sup>4</sup> 5 U.S.C. § 552a(o) et seq.

<sup>5</sup> 5 U.S.C. § 552a(e)(4).

## THE ADMINISTRATIVE PROCESS SHOULD INFORM THE PUBLIC ABOUT PRIVACY IMPACTS

A prominent theory behind the Administrative Procedure Act's enactment in 1946 was the idea of "scientific government." This was the notion that a band of impartial public servants would discover the one true public interest underlying legislation, and regulate in its service.<sup>6</sup>

Experience and modern scholarship reveal that the regulatory process, like the legislative process, does not locate some singular public interest. It responds to a cacophony of competing interests and values,<sup>7</sup> among which are the interests of regulators and bureaucracies themselves.<sup>8</sup> Administrative government does not improve on constitutional legislative processes so much as it improvises to accommodate the growth of the federal government in the latter half of the last century.

An increasingly prominent theory of the administrative process—though perhaps still a fallback from the idea that regulation would discern a "pure" public interest—is that it can open administrative lawmaking to public scrutiny,<sup>9</sup> particularly along lines that are deemed important by Congress. Several amendments to the APA in the last twenty-five years are consistent with this approach.

The Regulatory Flexibility Act,<sup>10</sup> passed in 1980, requires agencies to consider the special needs and concerns of small entities. Each time it publishes a proposed rule in the Federal Register, an agency must prepare and publish a Regulatory Flexibility Analysis describing the impact of the proposed rule on small businesses, organizations, government jurisdictions, and the like. The Initial Regulatory Flexibility Analysis is subject to public comment, and a final regulation must be accompanied by a final Regulatory Flexibility Analysis. The Reg-Flex Act apparently provides the model for the Federal Agency Protection of Privacy Act.

Along similar lines, Congress passed the Unfunded Mandates Reform Act<sup>11</sup> in 1995. Among other things, UMRA requires federal agencies to inform and work with states and localities on major regulations. The Small Business Regulatory Enforcement Fairness Act,<sup>12</sup> passed in 1996, requires agencies to work more closely with small business in formulating regulations. It also subjects the analysis requirements of the Regulatory Flexibility Act to judicial review.<sup>13</sup>

These laws provide extensive precedent for the Federal Agency Protection of Privacy Act. The federal administrative process has been modified several times to accommodate the interests of various private- and public-sector institutions. Opening that process to the privacy interests of individual Americans is a matter of consensus among a broad cross-section of advocacy groups and congressional leaders, as we see from the wellspring of support for this legislation.

## SOME IMPORTANT DETAILS AND NUANCES TO CONSIDER

The Federal Agency Protection of Privacy Act is modeled on the Regulatory Flexibility Act, which has been used with success for more than 20 years to get greater information about the impacts proposed regulations will have on small entities. Simply, the Act would require agencies to issue the same type of analysis—an Initial

<sup>6</sup> Stephen Breyer, *The Legislative Veto After Chadha*, 72 Geo. L.J. 785, 796 (1984) ("At the time of the New Deal, some believed that the agencies might develop a science of regulation, the canons of which would hold agency managers in check through their sense of professional discipline.")

<sup>7</sup> *Id.* ("Today, few believe, for example, in a science of ratemaking. . . . [W]e suspect that at best [administrative] procedures guarantee a fair result; and we are aware that a fair rate-setting or power plant siting process does not necessarily mean an economically sensible rate or an environmentally optimal plant location."); WILLIAM E. NELSON, *THE ROOTS OF AMERICAN BUREAUCRACY, 1830–1900* 86 (1982) ("[Today, we] . . . understand that so-called scientific analysis of facts cannot yield answers to legal, political, and ultimately moral questions that require difficult value choices."); MARTIN SHAPIRO, *WHO GUARDS THE GUARDIANS: JUDICIAL CONTROL OF ADMINISTRATION* 65–67 (1988) (discussing agency 'capture' and 'professional deformation' of bureaucrats).

<sup>8</sup> See WILLIAM A. NISKANEN, JR., *BUREAUCRACY AND REPRESENTATIVE GOVERNMENT* (1971) (building a plausible economic model of bureaucratic behavior around the assumption that bureaucrats act to maximize the budgets of their bureaus). Niskanen later refined his thesis to argue that bureaucrats maximize their bureaus' discretionary budgets. WILLIAM A. NISKANEN, JR., *BUREAUCRACY AND PUBLIC ECONOMICS* 36–42, 273 (1996).

<sup>9</sup> See George W. Gekas and James W. Harper, *Early Returns from Government Regulation of Electronic Commerce: What's New is What's Old*, 51 ADMIN. L. REV. 769, 795–99 (1999). This excellent article calls for further opening of the administrative process through standardized electronic rulemaking and public access to rulemaking information. *Id.* at 797–98.

<sup>10</sup> 5 U.S.C. §§ 601–612, Pub. L. No. 96–354, 94 Stat. 1164–1170.

<sup>11</sup> 2 U.S.C. § 1501.

<sup>12</sup> Pub. L. No. 104–121, 110 Stat. 856 (codified in scattered sections of 5 U.S.C.).

<sup>13</sup> See *Northwest Mining Assn. v. Babbitt*, 5 F. Supp.2d 9 (D.D.C. 1998); *Southern Offshore Fishing v. Daley*, 995 F. Supp. 1411 (M.D. Fl. 1998).

Privacy Impact Analysis—along with a notice of proposed rulemaking. After considering the comments of the interested public, agencies would have to issue a Final Privacy Impact Analysis along with the finally promulgated regulation.

The success of the Regulatory Flexibility Act increased with the addition of the judicial review provisions to the Reg-Flex law in 1996, and it is pleasing to see that the Federal Agency Protection of Privacy Act also would make agency action subject to judicial review. Knowing that judicial review is available will make agencies naturally solicitous of congressional intent without requiring a great deal of litigation.

As with all legislation, there are some elements that could be improved. The casual reader may suspect that the Federal Agency Protection of Privacy Act would require agencies to assess how private sector implementation of regulatory mandates would affect privacy. This reading is probably a stretch and, judging by the public statements you and your colleagues have made, Chairman Barr, this is not your intent. Rather, it appears that your intent is for agencies to assess the consequences of their own information practices on privacy.

Language perfecting the bill could require agencies performing an Initial Privacy Impact Analysis to “describe the impact of *the agency’s uses of information under the proposed rule on the privacy of individuals.*” (proposed 5 U.S.C. §553a(a)(1); suggested added language in bold). Likewise, agencies performing a Final Privacy Impact Analysis could be required to describe and assess “the extent to which *the agency’s uses of information under the final rule will impact the privacy interests of individuals.* . . .” (proposed 5 U.S.C. §553a(b)(2)(A); suggested added language in bold). These minor changes are one way to better express the intent of the legislation.

As you consider this legislation, you should be aware that it incorporates many policies beyond privacy. Security, for example, (made a part of Privacy Impact Analyses at 5 U.S.C. §553a(a)(2)(A)(iv) and 5 U.S.C. §553a(b)(2)(A)(iv)) is any number of practices and processes that respond to threats against a company or government’s ability to function. Only one such function is carrying out privacy obligations. A business or government that lacks proper security may well violate its privacy commitments, but may allow much worse to happen as well. The policy considerations that go into security of data in the hands of governments is a separate and significant issue beyond my expertise. There are benefits from requiring agencies to declare that they provide for security of personal information, as long as the agency is not so forthcoming as to breach security in the process.

Providing access and an opportunity to correct personal information is an important consideration (made a part of Privacy Impact Analyses at proposed 5 U.S.C. §553a(a)(2)(A)(ii) and 5 U.S.C. §553a(b)(2)(A)(ii)). But access and the opportunity to correct information go to fair treatment much more than privacy. Consider that there is no reason to access or correct information that will never be used. It is only important that information be correct if it may be used adversely to the interests of the individual. Using incorrect information against a person is unfair, not unprivate.

Access is also generally inconsistent with security. Giving access only to appropriate parties presents difficult security challenges clustered around authentication of identity. An Advisory Committee on Access and Security, convened by the Federal Trade Commission in early 2000, concluded its work without reaching consensus because of the complex interaction between these two, essentially conflicting, interests.<sup>14</sup> To illustrate this point: The privacy of information sealed in concrete and dropped to the bottom of the ocean is well protected, and it may remain private for eternity, but there is no opportunity to access it.

As with security, there is no harm in requiring federal agencies to inform the public of access and correction rights. Similar fairness protections are found in the Privacy Act of 1974, which obviously deals with more than privacy.

Using information for additional purposes (a part of Privacy Impact Analyses at proposed 5 U.S.C. §553a(a)(2)(A)(ii) and 5 U.S.C. §553a(b)(2)(A)(ii)) may affect privacy, depending on whether there is further disclosure of information. Information about a citizen’s medical condition and address, for example, collected for making health care payments, may not be rendered less private if the same part of the same agency uses that information to research whether people with certain conditions reside in certain areas of the country. If a subsequent use of information involves sharing that information with a state agency or a different federal agency, however, then the subsequent use can be said to render the information less private than it was before.

More importantly, though, a Privacy Impact Analysis that claims there will be no further sharing of information may provide false assurance. This is because nothing

<sup>14</sup>Federal Trade Commission, *Advisory Committee on Online Access and Security* Web page <<http://www.ftc.gov/acoas/index.htm>>.

prevents governments from changing the rules about their use of information after it is collected.

The National “New Hires” Database is an excellent case in point. The Personal Responsibility and Work Opportunity Reconciliation Act of 1996<sup>15</sup> required the Secretary of Health and Human Services to develop a National Directory of New Hires. This directory is a database of information on all newly hired employees, quarterly wage reports, and unemployment insurance claims in the United States.

The purpose of this new database was entirely laudable—helping states locate parents who have skipped out on their child support obligations. But, already, the data is being repurposed. The National Directory of New Hires has been expanded to track down defaulters on student loans. Additional expansions have been proposed that would give state unemployment insurance officials access to the database.

In the better view, privacy in information is lost when it is submitted to government authorities. Unlike in the private sector, there is no higher authority to which Americans can appeal when personal information held by governments is put to new and unanticipated uses. A Privacy Impact Analysis that claims there are protections against use of information for changed purpose may be accurate for weeks, months, or years. But this is weak protection compared to contractual obligations formed in the private sector. Privacy-protecting contracts may be regarded as permanent because their breach is contrary to legally enforceable obligations that neither of the parties can unilaterally change.

This does not counsel against requiring Privacy Impact Analyses to discuss use limitations. Such analyses may make Americans more aware when commitments to restrict uses of information are changed by subsequent Congresses and Administrations. We will be better informed if the Federal Agency Protection of Privacy Act is passed with all its current provisions.

This discussion of the many nuances of the bill is intended to illustrate the enormous complexity of information policy, and to caution against unconsidered adoption of the so-called “Fair Information Practices.” Often touted by pro-regulation privacy activists, they represent a vast array of different policies. Some are related to privacy; some are inconsistent with it. One does not have to agree with the baggage-laden concept of “Fair Information Practices” to support the Federal Agency Protection of Privacy Act.

The concept of “Fair Information Practices” appears to have originated in the early 1970s from a committee convened within the Department of Health and Human Services called “The Secretary’s Advisory Committee on Automated Personal Data Systems.”<sup>16</sup> The intellectual content of its report, commonly known as the “HEW Report,” formed much of the basis of the Privacy Act of 1974 and its thinking is useful for controlling government data collection and use.

The report treated the public and private sectors identically despite the vast differences in rights, powers, and incentives that exist in these different worlds. For this reason, it cannot be said that the HEW Report addressed all the complexities of the privacy issue. “Fair Information Practices” do not apply well to the commercial world. As an analysis of government information practices, however, the HEW Report was an important project and document. It also tells us that computers and privacy are not a new concern to Americans.

#### Conclusion

Again, Chairman Barr, Mr. Watt, and Members of the Subcommittee, congratulations on engaging an issue where you can truly improve the quality and character of life for all Americans. There is widespread consensus that people in the United States want to protect their privacy from government encroachments. The Federal Agency Protection of Privacy Act will inform the public about the privacy impacts of federal regulations, and empower them to make informed decisions about government programs. There are many nuances to consider and understand—privacy and information policy are very difficult areas—but the legislation you have proposed is an appropriate, measured, and important step in the pursuit of enhanced privacy protection for American citizens.

Mr. BARR. Thank you very much, Mr. Harper.  
Mr. Mierzwinski.

<sup>15</sup> Pub. L. No. 104–193.

<sup>16</sup> See Secretary’s Advisory Committee on Automated Personal Data Systems, *Records, Computers and the Rights of Citizens*, Department of Health, Education, and Welfare [now Health and Human Services] (July, 1973) <<http://aspe.os.dhhs.gov/datacncl/1973privacy/tocprefacemembers.htm>>.

**STATEMENT OF EDMUND MIERZWINSKI, CONSUMER PROGRAM DIRECTOR, UNITED STATES PUBLIC INTEREST RESEARCH GROUP**

Mr. MIERZWINSKI. Thank you, Chairman Barr, Mr. Watt, Members of the Committee. It is a pleasure for U.S. PIRG to join my colleagues in supporting your important legislation, the Federal Agency Protection of Privacy Act.

The State Public Interest Research Groups have had a long-standing interest in privacy. We consider privacy to be an important public policy issue. Privacy decisions by Government agencies affect consumers in both their private lives as consumers and in their public lives as citizens.

We are pleased to support the bill. Its establishment of procedures for agencies to conduct privacy impact analyses and to consider the privacy interests of individuals throughout the rule-making process achieves two important goals.

First, it will require agencies to consider and compare various data collection schemes and describe their impacts. This very process by its very nature will require bureaucrats to consider less privacy-invasive alternatives to their typical rote proposals.

Second, the bill will shine sunlight on the rulemaking process. As the noted privacy champion and Justice Louis Brandeis said, "sunlight is the best disinfectant." The bill will offer consumers and citizens an earlier chance to review and analyze rulemaking proposals by agencies that could allow or require collection of personal information.

Currently, under the Privacy Act, the system of record notices have become boilerplate. They provide valuable but very stylized information to data subjects. Your bill will require more information to be disclosed, and it will require it to be disclosed in a readable manner for consumers and it will be disclosed earlier in the regulatory process so that it will have an effect on the regulatory process, again, rather than just being a piece of boilerplate. And again, as my colleagues have pointed out, your bill accomplishes all this in a narrow way without overly burdensome requirements on agencies because it uses familiar rulemaking processes.

We particularly applaud the provision requiring a periodic review of agency rules that have a significant impact on privacy. Many of the agencies that are covered under the Privacy Act have significantly changed the ways that they collect and use information and match information and share databases over the last 25 years. Yet, they haven't changed their privacy policies significantly. Periodic review is an important provision of the legislation.

We would suggest the following amendments to the legislation to make a good bill even better.

We believe that you should make reference to all of the original fair information practices, as proposed in 1973 by an HEW task force and then embodied into the 1974 Privacy Act. While your bill builds on the FIPs, a direct reference to the FIPs and clarification that its intent is to rely on all of the FIPs, we think, would strengthen the bill immeasurably. If it is not appropriate to mention these fair information practices in the legislation itself, reference them in the Committee report as an alternative.

Second, we would urge you to take the privacy impact analysis that is required to be published in the Federal Register and specifically require agencies to publish it on their Web site. Consumers and citizens don't read the Federal Register. Washington lobbyists read the Federal Register. I think that the bill has very important disclosure provisions, but a specific reference to the Web sites will force the agencies to do the right thing.

The fair information practices are discussed in some detail in my written testimony. They have been adopted by the OECD. They have been endorsed by the Reagan administration and by the Clinton administration. I want to point out that an unfortunate by-product of the increased interest in privacy that has occurred in the last several Congresses is that business groups, and even the Federal Trade Commission, have developed what I call FIPs-light proposals.

Notice and opt-out has been described as a summary of the fair information practices, and as we all know, fair information practices are much more sophisticated and robust than simply providing notice of privacy policies and giving consumers a limited right to say no to some sharing practices.

Some of the problems that some of the other witnesses have discussed are also referenced in my testimony. Familiar customer proposal—200 to 300,000 citizens complained about this proposal which would have required immense data surveillance on the lives of ordinary bank customers. I think that that is one example of legislation which would have benefitted tremendously from your legislation.

Finally, I want to point out that some agencies, under the auspices of the Chief Information Officers Association of the Federal agencies, have already taken it upon themselves to make privacy impact analyses a best practice. We think it would be even better practice for the Congress to codify your legislation and make privacy impact analyses the law.

Thank you very much.

[The prepared statement of Mr. Mierzwinski follows:]

#### PREPARED STATEMENT OF EDMUND MIERZWINSKI

Chairman Barr, Rep. Watt, and members of the committee: Thank you for the opportunity to testify before you on the important matter of privacy protection. As you know, U.S. PIRG serves as the National Association of State Public Interest Research Groups. PIRGs are non-profit, non-partisan public interest advocacy organizations with members around the country. The state PIRGs have a longstanding interest in privacy. We consider privacy to be an important public policy issue. Privacy decisions by government agencies affect consumers in both their private lives as consumers and public lives as citizens.

U.S. PIRG is also a founding member of the Privacy Coalition<sup>1</sup>, established in 2001 by a broad range of consumer, privacy, civil liberties, family-based and conservative organizations that share strong views about the right to privacy. The groups had previously worked together on a more informal basis in opposition to the intrusive Know-Your-Customer rules and in support of financial privacy proposals offered in the 106th Congress by members of the Congressional Privacy Caucus.

#### SUMMARY:

U.S. PIRG is pleased to support, with suggested amendments below, your proposed legislation, The Federal Agency Protection of Privacy Act, HR 4561. Its estab-

<sup>1</sup> See <http://www.privacypledge.org> for the coalition's principles, endorsers and other information.



lishment of procedures for agencies to conduct privacy impact analyses and to consider the “privacy interests of individuals” throughout the rulemaking process will achieve two important goals in those circumstances where its provisions must be complied with.

—First, it will require agencies to consider and compare various data collection and use schemes and describe their impacts. This very process will, by its nature, require bureaucrats to consider less-privacy invasive alternatives to their typical rote proposals.

—Second, the bill will shine sunlight on the rulemaking process. As the privacy champion and Justice Louis Brandeis once said—“sunlight is the best disinfectant.” The bill will offer consumers and citizens a chance to review and analyze rule-making proposals by agencies that could allow or require the collection or use of personal information. The current provisions of the Privacy Act requiring system of records notices have become boilerplate publications that provide valuable but highly stylized information to data subjects or others interested in the process. Your bill is important because it will require disclosure of more information about the privacy impact of agency proposals and will provide more context for those proposals than the disclosures under the Privacy Act. Also, Privacy Act notices usually are published late in the administrative process, after most or all of the decisions have been made. Your bill will force agencies to consider privacy at an earlier stage of rule-making and will require them to offer public notice and consider public comments.

Your bill accomplishes all of this using a familiar rulemaking process that does not impose undue burdens on agencies.

We applaud the provision requiring a periodic review of agency rules that have a significant impact on privacy. Experience under the Privacy Act of 1974 demonstrates that agencies rarely review their activities that affect privacy. Even though information technology has produced massive changes in agency operations, many agencies operate under privacy policies that have not been reconsidered for many years. Periodic review is a crucial feature of the legislation.

We would suggest the following amendments to improve the proposal.

—First, we urge you to make reference to all of the original Fair Information Practices (FIPs), as proposed in 1973 by a Health, Education and Welfare (HEW) task force and then embodied into the 1974 Privacy Act. The Privacy Act of 1974 already reflects all FIPs principles, and a reference to FIPs in your proposal will not add any new requirements. While your bill builds on the FIPs, a direct reference to the original FIPs, and clarification that the bill’s intent is to rely on all FIPs principles would strengthen the bill immeasurably. If it is not appropriate to mention FIPs in the legislation itself, then a reference in the committee report would be an alternative.

—Second, the bill calls for the publication of an initial privacy impact analysis in the Federal Register. We suggest that the Federal Register publication be supplemented by publication of the privacy impact analysis on the agency’s website. It might also be suitable to require agencies to maintain a privacy impact analysis page on their websites to centralize all privacy impact analysis activities in one place. In general, the procedures specified in the bill for gathering public comments are good, but a specific reference to the Internet would be helpful.

—Third, in several places, the bill refers to the goal of preventing information collected for one purpose from being used for another purpose. We suggest that this language be amended to say “from being used OR DISCLOSED for another purpose.”

#### THE FAIR INFORMATION PRACTICES:

Data collectors have an obligation to conform their data collection practices and systems of records to Fair Information Practices (FIPs), which were originally proposed by a Health, Education and Welfare (HEW) task force and then embodied into the 1974 Privacy Act<sup>2</sup> and also the 1980 Organization for Economic Development and Cooperation (OECD) Guidelines<sup>3</sup>. If data collectors do not conform their data

<sup>2</sup>Noted privacy expert Beth Givens of the Privacy Rights Clearinghouse has compiled an excellent review of the development of FIPs, “A Review of the Fair Information Principles: The Foundation of Privacy Public Policy.” October 1997. <http://www.privacyrights.org/AR/fairinfo.html> The document cites the version of FIPs in the original HEW guidelines, as well as other versions: Fair Information Practices U.S. Dept. of Health, Education and Welfare, 1973

<sup>3</sup>For a comprehensive manual of major U.S. and international privacy laws, treaties and other agreements, see the “The Privacy Law Sourcebook 2001: United States Law, International Law, and Recent Developments”, edited by Marc Rotenberg, 2001, Electronic Privacy Information Center, Washington, DC <<http://www.epic.org/bookstore/pls2001/>>

systems to Fair Information Practices—use limitation, right of review and correction, and procedures to ensure accuracy and security while preventing secondary use without consent—then data subjects face privacy perils. The OECD version of FIPs was endorsed by both the Reagan Administration in the early 1980s and again by the Clinton Administration in the mid-1990s.

While the Privacy Act of 1974 applies only to federal agencies, some privacy laws affecting the private sector, such as the Fair Credit Reporting Act<sup>4</sup>, also generally adhere to its principles. It is important that the committee understand that over the last several decades, numerous alternative, weaker versions of the FIPs have been suggested, especially with the heightened interest in privacy that has developed in the Congress over the last several years. Most of these recent proposals could at best be called “FIPs-Lite” and at worst could be called anti-privacy proposals or even privacy prevention proposals. The Federal Trade Commission’s 1998 version of FIPs is a good example of a casual restatement that leave out or modifies important elements.

The bill, for example, could be improved in the following way: In its description of the contents of a “final privacy impact analysis” it refers to “notice of the collection of personally identifiable information.” Notice is not enough. The Fair Information Practices require collection limitation and also require purpose specificity. Data collectors have access to more information, more matching programs, and more powerful technological tools and computer memory than ever before. Unless restrained, they will collect and analyze information for no other reason than the (perhaps apocryphal) reason that the noted explorer Mallory is said to have given for attempting to climb Mt. Everest: “Because it is there.” Your bill should not diminish the Fair Information Practices to suggest that notice of collection is adequate practice. Data collectors in the public and private sectors should define the purpose of collection and collect data for defined and limited purposes.

Other FIPs principles worthy of reference and should not be overlooked are: 1) the data quality principle, which provides that personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete, and kept up-to-date; and 2) the accountability principle, which provides that record keepers should be accountable for complying with measures which give effect to FIPs principles.

We would be pleased to work with the committee to strengthen the bill’s relationship to the original Fair Information Practices.

#### RECENT PROPOSALS THAT COULD HAVE BENEFITED FROM PRIVACY IMPACT STATEMENTS:

In our view, numerous rulemakings have privacy implications for consumers and citizens. In some cases, government may propose to establish or modify governmental programs affecting “citizen” data subjects and personal information about them. In other cases, proposed government rules may require private firms to collect information on “consumer” data subjects, for government purposes. The proposed legislation’s requirements could reduce privacy impacts. Two recent examples are the following:

—Several years ago, after receiving 200,000 citizen comments, financial regulators considered and withdrew sweeping “Know Your Customer” regulations designed to curb money laundering, although certain provisions of Know Your Customer were approved in a narrower form.<sup>5</sup> That proposal would have imposed a massive new regulatory requirement on financial institutions to track the transactions of ordinary customers and report a number of new “suspicious” activities. Yet, just last week, in response to requirements of the USA Patriot Act of 2001, financial regulators announced a major expansion of money laundering requirements<sup>6</sup> under the same Bank Secrecy Act requirements. Without in any way diminishing the important anti-terrorism intent of the new rules, we would note that both these proposals would have benefited from review under your proposed law. The proposed and par-

<sup>4</sup> 15 USC 1681 *et seq*

<sup>5</sup> “Crucial to maintaining the confidence of bank customers in our banking system is their expectation that their relationships with their banks will be private and confidential—that information they provide to their banks will not be used for ulterior purposes; that transactions will be processed objectively and nonjudgmentally; and that the interests of the customer will be paramount in importance,” said Comptroller of the Currency John D. Hawke Jr on 4 March 1999 in withdrawing the proposal. See <<http://www.occ.treas.gov/ftp/release/99%2D17.txt>>.

<sup>6</sup> See Title III of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 (Public Law 107–56). Title III of the Act amends anti-money laundering provisions of the Bank Secrecy Act (BSA), subchapter II of chapter 53 of title 31, United States Code. These amendments are intended to make it easier to prevent, detect, and prosecute international money laundering and the financing of terrorism.

tially-withdrawn Know Your Customer rule and the new money laundering rules both require banks, credit card companies and other financial firms to conduct sweeping surveillance of ordinary accountholders. As the Free Congress Foundation has noted, some parts of the new rules make a great deal of sense, while others may not.<sup>7</sup>

—In 1999, the Health Care Financing Administration established the OASIS program (Outcome and Assessment Information Set.). HCFA wanted home health care providers to conduct a 19-page survey when enrolling a new patient and then every 60 days until services conclude. In addition to collecting basic identification and medical information, the survey originally asked whether patients are depressed or feel a “sense of failure.” It asked if patients have attempted suicide, exhibited “inappropriate behavior” or made any “sexual references” during conversations. It also asked for personal financial information. Publicity eventually forced a cutback in the survey, but the public debate came from press coverage rather than from full, advanced, and public disclosure by the agency of its intentions.<sup>8</sup>

#### CONCLUSION

Some steps have already been taken to implement the concept of Privacy Impact Analyses by government agencies. For example, a committee of the Chief Information Officers of federal agencies, in 2000, made development of Privacy Impact Analyses a criterion in determining “best practices.” The Internal Revenue Service PIA serves as a useful model.<sup>9</sup> However, we urge codification of the concept, through enactment of HR 4561 with suggested amendments.

Thank you again for the opportunity to testify before the committee on this important legislation. We look forward to working with you on its passage.

Mr. BARR. Thank you very much, Mr. Mierzwinski, and I appreciate all Members of the Committee for their statements and would ask all of you if there, as we have heard from at least a couple of the witnesses, specific areas in which we can strengthen the legislation, please get that information in whatever detail you are able to us so that we can see if there are some ways that we can strengthen the legislation, while not going so far as to engender sufficient opposition so that it kills the legislation. That is, of course, the very difficult balancing act that we have on this and any piece of legislation, usually in direct or inverse proportion to the validity of the legislation.

What I will do now is recognize myself for 5 minutes for questions, and then turn to other Members of the panel, and hopefully we will have another round of questions because I know I have a lot more than we can get to in just one round. But we may also submit additional questions in writing if we are not able to get to them all today, and I would ask you all’s cooperation in reviewing those expeditiously and getting the answers back to us so that we can again incorporate all of that into the record.

As I think everybody has testified, this is indeed a very modest piece of legislation. But as we all know also, the most powerful force in the universe being the force of the status quo, we know

<sup>7</sup> In a release, Free Congress Foundation noted: “We need to raise the concern of consumers about the privacy of their personal and sensitive financial information. Not only will the new regulations prove ineffective against terrorism, but they represent an added threat to a consumer’s privacy by allowing easy access by government authorities to the financial transactions of consumers.” It then pointed out that the proposed “financial services hotline which will allow financial services employees to quickly report suspicious transactions . . . [is] more sensible than burying law enforcement in reams of paperwork that requires a huge investment of time to shift through what are mostly routine financial transactions.” See statement of J. Bradley Jansen, Free Congress Foundation, 25 April 2002, <<http://www.freecongress.org/press/releases/020425.htm>>

<sup>8</sup> Citations: U.S. to Start Gathering Patient Data Care Survey Draws Privacy Objections By Robert O’Harrow Jr. Washington Post, Thursday, March 11, 1999; Page A01; Under Fire, U.S. Amends Plan to Collect Health Care Data By Robert O’Harrow Jr. Washington Post, Thursday, April 1, 1999; Page A05

<sup>9</sup> See <<http://www.cio.gov/Documents/pia—for—it—irs—model.pdf>>

that even this very modest piece of legislation will engender opposition by the status quo.

If each one of you could take just a minute or so to speculate with me and give me your ideas on what will be the likely arguments that we will hear from the forces of the status quo; that is, executive agencies when they see this legislation.

And, Ms. Waters, if you could start, and then like I say, I will take my entire 5 minutes if each one of you could just comment briefly on that, looking down the road, what you think the arguments are going to be by the executive branch as to why we shouldn't pass this radical piece of legislation.

Ms. WATERS. Well, I think that one of their arguments may be it is going to add more words to the Federal Register, make it longer, and make their jobs more difficult, and that regardless of arguments that it is not going to be burdensome, I think that they will still try to make that argument of burden.

But also where do you draw the line? Which types of regulations would require it and which ones don't? If it is, you know, dealing with, you know, human research subjects or whatever, which regulations would require this impact statement and which ones would not, I think, might be one of their arguments.

Mr. BARR. Thank you.

Mr. Nojeim?

Mr. NOJEIM. Their arguments will likely revolve around the things that I said the bill does not do. So look to those "does not dos" for what the agencies will be arguing.

I am particularly concerned about arguments that we expect to be made against the judicial review provision in the bill. Agencies will argue that it will tie up their regulations for a long time. That is not true. The bill includes sufficient exceptions so that a judge could—even while finding that the agency had violated the provisions of the act, it could allow the agency to go forward with a rule-making procedure if it determined that that was in the public interest.

We think that judicial review is crucially important because, you know, nobody likes to have somebody look over their shoulder and tell them no, when forever they have been operating without a requirement or without that procedure in place.

This bill would put the judiciary in a position to tell agencies that they need to comply with very limited procedures that require them to consider privacy interests when they issue their regulations. We think that the agencies probably won't comply, or they won't comply adequately, unless that prospect of judicial review is maintained. So we think it is very important that you keep that in the bill and fight to keep it there.

Mr. BARR. And, again, do you see that as probably the major line of opposition?

Mr. NOJEIM. I think it is probably going to be one of the major lines, yes.

Mr. BARR. Thank you.

Mr. Harper?

Mr. HARPER. I can imagine two different arguments that might come up against this bill. One is that agencies will say we are already complying with the Privacy Act, that takes care of it, we are

protecting privacy. I think the appropriate response to that is that this bill does more. It causes there to be a national discussion about privacy, not just legal, technical compliance with a law that is obscure to most Americans.

The second argument I think that you will hear is that this is too much; it is too much to ask. That reveals, quite frankly, just how much personal data is being used by Federal agencies. And if you get that argument, that should steel your resolve to move forward with the legislation.

Mr. BARR. Thank you.

Mr. Mierzwinski?

Mr. MIERZWINSKI. Mr. Chairman, I agree with the other witnesses. I really think the agencies are going to say we are already doing this through the Privacy Act, we are already doing enough. And my response to that is, again, the bill does more things and requires different things, and I think you should reject those arguments.

Mr. BARR. Thank you.

Mr. Nojeim, if I could, I have just a few seconds left here, but you mentioned specifically in your testimony—and I was reading it, your written testimony, about law enforcement. Do you see—my view is that this will not affect law enforcement in any way, shape, or form.

Do you see any potential areas where a legitimate argument could be made by law enforcement agencies that this will hamper their efforts to properly investigate and enforce and prosecute our criminal laws?

Mr. NOJEIM. No, it won't hamper efforts to investigate and prosecute people who they believe are criminals. What it will do is require law enforcement agencies, just like every other agency, to explain the privacy implications of the regulations they propose. That will not stop them from proposing regulations that would have an adverse effect on privacy and from adopting those regulations, but they do have to consider alternatives. That is what this bill is about.

Mr. BARR. Thank you.

I recognize the gentleman from North Carolina, the distinguished Ranking Member, for 5 minutes.

Mr. WATT. Thank you, Mr. Chairman. I actually have several different lines of inquiry that I wanted to go into, and I am not sure which one I want to pursue the most. I guess I want to start by commending Mr. Harper for taking the—making the effort to define privacy.

It is quite a fascinating description that you have given about how you define it, and I have a whole bunch of questions that I could address to that issue as kind of a tangential issue.

I assume that the definition of privacy that you have proffered is kind of an academic effort to get a definition out there in the marketplace, but really is not going to have any substantial implications for this bill one way or another, or will it?

Mr. HARPER. I worked on defining privacy because I have been troubled with how privacy has been discussed in public debate. Identity fraud is arguably much better approached as a serious crime problem than as a privacy problem. Spam is a problem—un-

solicited commercial e-mail is a problem that is a serious inconvenience and annoyance based on marketeers not knowing anything about who they are trying to reach, which is very different from the traditional perspective of privacy, which is too much information about consumers being available.

So I have worked through what is essentially a legalistic definition of privacy; that is, that privacy is a subjective condition people enjoy when they first have legal power to control how information is shared, and, second, exercise that power consistent with their values and interests.

That is a definition of privacy that doesn't attempt to place my own privacy preferences or interests on other people's. It is a definition that is neutral and allows individual consumers and actors to define for themselves.

Mr. WATT. What implications, if any, will that definition have for this bill, as you see it?

Mr. HARPER. I suspect that it can help enlighten the legislative history, help to improve the discussion and debate on the bill. But as far as the substance, for instance, going to judicial review, the definition of privacy I have offered would never make it into judicial review of the legislation.

Mr. WATT. I think I agree with you because it is too—it is a moving target.

Mr. HARPER. Exactly, yes.

Mr. WATT. But let me go on to something else.

Ms. Waters, in your testimony I couldn't help—it kind of triggered, some of the things you said, a question about this electoral reform bill. Both the House bill and the Senate bill right now have provisions in them that will require some kind of voter identification, one of the things that I am deeply troubled about in both pieces of legislation, and many of the interest groups are deeply troubled about.

I take it that your analysis related to Social Security numbers and the uses and abuses that have been made of them would be equally applicable, or could be equally applicable to those kind of voter I.D. requirements that are in those bills.

Are you familiar with those requirements, first of all?

Ms. WATERS. I am a little bit aware of what has been discussed about the use of Social Security numbers specifically in terms of voter identification. And really the larger problem here is—like I mentioned in my testimony, is the over-uses of a Social Security number, something that was originally never intended to be an identifier, and now it is used at every—at the drop of a hat. It comes down to how much—

Mr. WATT. Are those proposals troubling to you?

Ms. WATERS. It is troubling to me when you expand the use of the Social Security number because, again, it comes back to how much information do you need to provide to guarantee who you say you are, and the Social Security number has become our national I.D. number.

Mr. WATT. And has your organization expressed its concerns about that in this voting reform context?

Ms. WATERS. During the Senate debate, we did express concern prior to—I think it was Mr. Kyl's office who had talked about the

use of the Social Security number, and we did express our concern about that. And so it is—it has become our unique identifier.

Mr. WATT. And I know Mr. Nojeim's organization has been pretty aggressively expressing its concerns about this in the voting context. I assume you are concerned about those implications, also.

Mr. NOJEIM. Yes. We see requirements of Social Security numbers and of I.D. cards both as obstacles to voting that will have a disproportionate effect on minority voters.

Mr. WATT. I want to be the first to acknowledge that this really has little to do with this bill, but it is nice to get on the record publicly some of the concerns that people are expressing and hope to build a wider and bigger coalition to express those concerns in the voting reform context, too. So I am using this opportunity for that purpose.

I think my time has expired. I have got one more area that I want to go into that more directly relates to this bill, but I think the Chairman is planning to come around again so I will get to that on the next go-around.

I yield back the balance.

Mr. GEKAS. [Presiding.] We thank the gentleman.

The Chair yields to itself 5 minutes for a group of questions.

As you could tell by my opening statement, I was concerned and pleased with the inclusion in this bill—in fact, that was the most attractive feature to me as I became a cosponsor of it on judicial review.

The law school articles and the law—what do we call them—the articles that are written about it all hark back to the actions that we took under SBREFA, in which we were amending the Regulatory Flexibility Act to provide judicial review.

And one of the concerns that Mr. Nojeim uttered just a while ago was that the criticism of judicial review back then and now is cost of it and delay and complexity that it might create. But just the existence of judicial review is a tremendous safeguard, and I am almost tempted to say the devil with the cost and the complexity; we need judicial review.

This thought that I want to express now I wanted to subject to your thinking. If we pass this bill and it becomes law—and in it will be, of course, substantial judicial review—isn't it a fact that a flurry of cases then that would come under it in the near and far future would so compact the issue that there will be less judicial review after lawyers and others and the agency heads look at the case law and its results? Therefore, judicial review will be less current or less used than before.

Do we comport with that kind of general view?

Mr. NOJEIM. I think that if there was a flurry of cases at the front end that that would be the result. Agencies would learn what works, what the courts would accept, and they would just adapt as a matter of routine.

I question, though, even whether there would be an initial flurry of cases in the first place because if the bill provided for a substantive right to require the agency to make a particular pro-privacy choice, I think then you would see a lot of litigation. But the bill only requires following very limited procedures, so if there was a flurry of litigation, I think it would be at the front end then it

would die down. But I really doubt that there would even be that initial flurry. I do think, though, that without the judicial review, agencies would not comply with the procedures that are required.

Mr. GEKAS. Mr. Harper?

Mr. HARPER. I am going to have to go from memory on this, and I just recently read an article about SBREFA and the existence of judicial review and I believe there were five cases after SBREFA brought judicial review to the Reg Flex Act. I don't think you can quite characterize that as a flurry. That is enough for a close-knit community, the agencies, which are constantly watching administrative procedure cases—that is enough for them to learn what is expected of them under the judicial review provisions; again, not a flurry, just enough to get everybody into line and understanding the nature of the law.

Mr. GEKAS. Does anybody else have any comment on that?

I have no further questions with respect to the specifics in the bill. I just want the record to indicate that the question of judicial review under SBREFA on which I relied as one member for approbation of the judicial review in this legislation was based in part on articles written in the William and Mary Law Review by one Jeffrey J. Pollick, P-o-l-l-i-c-k, and they consolidate my thinking on judicial review and I am very satisfied to be a cosponsor of the legislation.

Jim?

Mr. HARPER. If I can just make two related comments, first I appreciate that you took less of the opportunity that you had to put me on the spot with this kind of question.

Mr. GEKAS. Yes.

Mr. HARPER. But I also want to put you on the spot briefly and remind everybody here that it was a hearing you held on the "know your customer" rules where the Comptroller of the Currency stated that he would withdraw those rules after a lot of agitation from, I believe, everyone at this table. This has been—looking at the administrative process, this has been a pro-privacy Committee for a long time, partly under your chairmanship.

Mr. GEKAS. I thank the gentleman.

The time of the Chair has expired. The Chair asks the Chair to resume the Chair.

Mr. BARR. [Presiding.] I apologize for having to leave for a couple of minutes, but appreciate the distinguished former Chairman for reassuming the Chair.

At this time, I would like the record to reflect that we have been joined by our distinguished colleague from California, Mr. Issa, and recognize him for any opening statement he might care to insert into the record and for 5 minutes of questions.

Mr. ISSA. Thank you, Mr. Chairman, and I will waive substantially both. I will be honest. Even though I have a strong interest in this, I am, for once, not decided and trying to learn more about a bill. I know everyone is going, "Issa in doubt?" But it does happen on occasions.

I do think that we have a great task ahead of us, particularly with the Supreme Court weighing in on this industry, the Administration trying to regulate within its existing powers, to figure out where and when we should push in new initiatives. And I have



some learning to do on this particular one, but in general I want to be supportive of efforts to ensure that in this new era we have no less privacy than we had before and, if possible, perhaps a little more.

So, Mr. Chairman, I will do what I never do, which is shut up and listen. Thank you.

Mr. BARR. Well, we hope that in so doing we can move you from the undecided to the favorable column on the legislation. We appreciate very much the work that you have done and continue to do on these very important matters, Mr. Issa.

Since there are no other Members to ask questions, what we will do now is turn to round two as long as the witnesses—can you all stay for just a short while longer? We appreciate that. We are lucky today. We haven't had any votes, so we will press our luck a little bit here.

I will recognize myself for 5 minutes, and then the distinguished Ranking Member.

I was intrigued also in reviewing your written testimony, Mr. Nojeim, and I think the other witnesses have alluded to some of these matters also, some "good government" programs or worthwhile regulations or laws that just sort of get away from us once they are enacted.

And I was particularly interested in the anti-money laundering statute and regulations that you talk about in some length in your written testimony, Mr. Nojeim. A good idea. In other words, the Government should be able to track true money laundering, but SAR, suspicious activity, reports and other mechanisms, and now, as you indicated, the Treasury working on additional regulations to become involved in monitoring the activities of those who deal in precious metals, jewels, pawnbrokers, loan or finance company, private bankers, insurance company, travel agency, telegraph companies, real estate brokers, and others.

Would this legislation be able—if it were enacted, would it be able to in any meaningful way stem the tide of these sort of gradual encroachments? I don't think that we are going to face an Exxon Valdez, as Mr. Harper indicated. It is more like just a very, very gradual usurpation, and all of a sudden we wake up 1 day and the Exxon Valdez is there, but it has been over a period of time; the old analogy of, you know, you throw a frog into a vat of boiling water and he or she is going to jump out right away. But if you throw the frog into a vat of water that is, you know, cool and then you gradually heat it, pretty soon it is just dead by gradual encroachment. I think that is what we are seeing here.

But would this—specifically looking at your example, Mr. Nojeim, of the way the anti-money laundering effort has sort of gotten away from us now and is just getting, you know, more and more intrusive, would this legislation afford any meaningful relief with this sort of scenario?

Mr. NOJEIM. The problem with the money laundering legislation that is being implemented now is that it requires the reporting of primarily innocent transactions. I mean, the suspicious activity reports—maybe 1 percent, maybe 2 percent of them actually result in some kind of indictment or criminal action.

On the currency transaction reports, millions, millions of reports of transactions of \$10,000 or more result in very, very, very few, relative to the numbers, criminal indictments. So what you have is a system that primarily tracks the flow of money, as opposed to tracking criminal activity.

The bill will not reach backward; it will not reach backward for regulations that have already been adopted. But in cases where the agency is charged with or is looking at expanding the reporting requirements to new industries after the bill is passed, it will have, I think, a good effect. It will require the agency to determine whether there are alternatives to collecting all this information, whether it could be more efficient and less invasive of privacy. So I think it would have that beneficial effect, but only looking forward, not looking back.

Mr. BARR. So it is not going to take the place of good legislation. We need to look at these things when the legislative proposals first come to us. This is not going to be a substitute for Congress doing its job in the first place.

Mr. NOJEIM. Well, Mr. Chairman, in the future maybe we will look at legislation that would require Committees to include in their Committee reports a privacy impact statement. We already see in some Committee reports an estimate of how much the bill will cost. Maybe we need an estimate of how much the bill would cost in terms of privacy. I don't think that is something that we could do today, but it is something that we might look forward to in the next session.

Mr. BARR. I like that.

Ms. Waters, I don't recall specifically whether you touched in your oral testimony on the national I.D. and, you know, this trusted flyer. I know that several of you all have when we have talked about this on a number of occasions.

Would this proposal, would this legislation—presuming that some sort of national I.D. or standardized drivers' licenses or trusted flyer program that is not already enacted as a matter of law before this legislation can be, would this legislation afford some relief in stopping those sorts of proposals?

Ms. WATERS. Most definitely. And just today, I believe that your colleagues, Mr. Moran and Mr. Davis, are going to be introducing a bill on standardizing a driver's license. We need to make sure that through the regulatory process that this doesn't turn into something greater than what it was intended to do of making drivers' licenses more secure.

Mr. BARR. We can presume, though, that it will unless it is stopped, I think, correct?

Ms. WATERS. It is a concern, and we haven't, you know, seen the text of the bill yet, but we are going to have to be really careful as we consider these types of proposals because technology has gotten way ahead of the law. And when it comes time to implement some regulations, there could be some unintended consequences down the road, just as there were with the Social Security number.

Mr. BARR. Thank you.

If I could request Mr. Watt's indulgence to just ask one more question before I relinquish the microphone, again I forget who it

was—who has done some work on red light cameras? Is that yourself, Mr. Harper?

Mr. HARPER. Yes.

Mr. BARR. Would this legislation—if it were enacted, would it provide some relief to stopping the implementation of red light camera policies, or the establishment of red light cameras at least by Federal agencies? Would that be something that would trigger the procedures under this law?

Mr. HARPER. The major limitation on its ability to do that is the fact that a lot of red light camera programs are State and local programs rather than Federal programs. But, for example, where the National Park Service is doing this, I believe they would have to reveal their personal information collection, for example, of drivers' licenses, the images of drivers, that kind of thing. Again, it would reveal what the information practices are of the agency so that that can be a part of a more robust debate about red light cameras.

Mr. BARR. Thank you.

Mr. NOJEIM. May I add one more thing?

Mr. BARR. Sure.

Mr. NOJEIM. You couldn't stop the agency from doing the red light cameras. You couldn't stop the agency from adopting "trusted passenger." What you can do with this legislation is make the agency think twice, look at alternatives, the less privacy-invasive alternatives, and that in and of itself will encourage them to adopt the less privacy-invasive alternatives. But the bill again—

Mr. BARR. Or at least make it more difficult for them not to do that.

Mr. NOJEIM. Right, right, right.

Mr. BARR. Thank you very much.

The gentleman from North Carolina is recognized for 5 minutes.

Mr. WATT. The questions the Chairman has been asking and your responses have given us some good information to prepare for what I hope will be another hearing on this, at which the other side—Mr. Chairman, I think this is important to give the other side the opportunity to come and try to make the case that you have been kind of anticipating and the Chairman has been kind of anticipating that they will make.

So let me go one step beyond where the Chairman has gone and ask you, if you were putting together such a hearing, what would be the agencies that you would think you would have the most need to hear from and get their concerns out on the table so that we can try to address them and maybe assuage their concerns? What Federal Government agencies ought we be considering bringing to the table to testify and at least hearing whatever specious arguments they are going to give us?

Mr. HARPER. I will tell you that every agency has their share of databases. Maybe for purposes of a good hearing, you bring in one that everybody knows has a lot of financial information—Social Security Administration. Ask the Department of Interior. You wouldn't expect them to have databases, but I am willing to bet that they do. A cross-section of agencies—that would be my recommendation, because they have all got them.

Mr. NOJEIM. The good news about bringing in more agencies is that you will be able to not just hear their side, but there may well

be privacy breaches that our side might want to highlight when those agencies appear. You might want to bring the education agency, you might want to bring in OMB, and you might want to bring in the Justice Department.

Mr. WATT. Picking up on something else that the Chairman has raised—and I am doing this not for the purpose of undermining the bill but for the purpose of illustrating and making a point that I want to make, which is what is typically good for the goose is good for the gander, and if you don't believe in that in this area, then you are going to start meeting yourself coming and going.

One of the concerns that several people raised with me when I was considering the possibility of supporting this bill before I decided to support it was this is going to have some very serious implications for the Brady bill and gun control.

My response to that was, okay, so what? You know, if we are doing something in the area of privacy with reference to gun control or the Brady bill or some law, then we need to know that from a privacy perspective, too, just like we would need to know it if we were maintaining records still at the FBI about the civil rights movement. We would need to know that, and individuals within the civil rights movement.

So having kind of given that platform, do you see any implications here, adverse implications, for the Brady bill or any of the things that I think ought to be on a level playing field when it comes to individual privacy, but some people might want to draw a line one way if they are conservative and another way if they are liberal, so to speak?

Mr. NOJEIM. First, I think you have illustrated one of the things that agencies might try to come up with. They will want to be excepted. They will want to have an exception that covers what they do from what the bill would require, and I think that you have made a good, strong case for no exceptions. Apply it to everyone.

On Brady bill-type issues, you are right. I mean, the information is going to be—is gathered under the Brady bill and the question will be whether the information that is gathered is necessary for the law enforcement purpose, and it would require the Justice Department to make a determination about whether the information—particular information needs to be gathered or doesn't need to be gathered.

But, again, it wouldn't compel a particular outcome. It would compel consideration of alternatives, which is exactly what I think is the "good government" thing to come out of this legislation.

Mr. WATT. Any other responses to that question?

Mr. HARPER. I think the question holds the answer in its hands. You need to gore everybody's ox with something like this. Everybody is not going to like it and Mr. Nojeim points out, if somebody starts to go for a carve-out, somebody else is going to go for it and everybody is going to start, oh, but this policy is so important to you that we have got to give up on privacy on that point and we have got to—we don't have to worry about privacy on that point. But if you stick with it across the board, we will all be better off.

Ms. WATERS. I think it is quite telling that, you know, you have Eagle Forum and ACLU sitting right next to each other, and the NRA joined us—

Mr. WATT. You all look good together. [Laughter.]

Ms. WATERS. You know, it is great to be able to join my friend, Greg Nojeim, you know, at a hearing because these issues are important not just to Republicans or Democrats, as we have mentioned in terms of highlighting coalition. But the NRA did join us at the press conference, and I think this has an impact in all different fields. And I agree with the other witnesses that agencies will try and get their own individual exceptions, and it is often the exceptions that kill legislation or will cause the loss of support of organizations like ours.

If I could quickly just clarify something for you, Mr. Watt, on the previous questioning regarding Social Security numbers, we do support photo identification for voting, but not the use of Social Security numbers.

Thanks.

Mr. WATT. Well, now, you opened up a whole other keg of worms here. I don't know how you can get there without—but we will talk about that in another context.

Ms. WATERS. I will be happy to talk to you about that another time.

Mr. WATT. I will leave it on a positive note. The Chairman and I sit beside each other everyday, and you all look a lot better sitting beside each other than we do. I will tell you that.

Mr. MIERZWINSKI. If I could just add, Mr. Watt, that the State PIRGs are strongly with you on the voter registration issue, and we have been longtime supporters of the motor voter bill and trying to mitigate the provisions in that bill that would require excessive documentation of voters.

Mr. WATT. See how easy it is to get this panel disagreeing with each other? It doesn't take much, but that shows the very delicate issue that we are dealing with here and how important it is. I appreciate all of you being here.

Mr. BARR. I thank the distinguished Ranking Member.

Just two brief final questions. One is actually a comment, I think. We have not uncovered in our research on this legislation any State laws that do similar things. Are you all aware of any States that have a State statute that is similar to what we are trying to do here?

Mr. HARPER. I am not aware of any such statute. A lot of States have privacy acts, a lot of States have open records acts, and the tension between the two is just like the tension at the Federal level. None have specifically taken into account privacy in the regulatory process. Obviously, doing it at the Federal level would lead the States to do that themselves, and the ripple effect would be substantial for privacy at the State and local level as well.

Mr. BARR. Both ways. I think it would help us, also, if there were more of a concern and a visible, proactive approach by some States. And I know all of your organizations are very active at State level, also, and I would encourage you all to try and get some of your colleagues interested in working these issues and bringing them to the fore at the State level.

That will help in two ways. One, many of these databases and regulations are just as intrusive and problematic from a privacy

concern with State governments, and that would also help us up here to develop support for this legislation and similar legislation.

One final question. Mr. Mierzwinski, you talked in your testimony about fair information practices. Have those been embraced by the current Administration?

Mr. MIERZWINSKI. I am not aware whether or not they have, Mr. Chairman. I can look into that and get back to the Committee with my findings. But as I noted, President Reagan and President Clinton both endorsed the OECD guidelines that adopted the fair information practices. We have been encouraged by, of course, a lot of what the President has said about privacy, but I don't know that they have endorsed the full principles of the fair information practices as originally articulated in 1973.

Mr. BARR. I presume you haven't been encouraged, though, by their position on medical privacy, as recently articulated.

Mr. MIERZWINSKI. We haven't been encouraged by the medical privacy delays and changes, no.

Mr. BARR. So we have some work in that area, too.

Mr. HARPER. Just briefly on fair information practices, I want to refer you to my testimony where I discuss each of them as a separate information policy. I think it is important.

As I discussed with you, Mr. Watt, the importance of defining terms, defining each policy, each of the fair information practices represent an important information policy and sometimes conflicting information policies. So it is important to consider them carefully.

Mr. BARR. Thank you.

Before we adjourn, I would like to thank the members of the media that were here. We have some very distinguished members of the media from the New York Times and other publications and outlets. We very much appreciate their interest in this legislation as well.

Again, thank you all very much for being here today and if you have additional information, please get it to us as quickly as possible so that we can incorporate it into our further work, because we really do want to move this matter through as quickly as possible, given the fact that every day that goes by sees a further chipping away at what little privacy Americans have left.

Thank you all very much, and this hearing is hereby concluded.  
[Whereupon, at 11:50 a.m., the Subcommittee was adjourned.]

## APPENDIX

### MATERIAL SUBMITTED FOR THE HEARING RECORD



#### WASHINGTON NATIONAL OFFICE

Laura W. Murphy  
Director

122 Maryland Avenue, NE, Washington, D.C. 20002

Tel (202) 544-1681 Fax (202) 546-0736

Chairman Bob Barr  
Subcommittee on Commercial and Administrative Law  
Committee on the Judiciary  
United States House of Representatives  
2138 Rayburn House Office Building  
Washington, DC 20515-6216

May 28, 2002

Dear Chairman Barr:

Thank you for providing me the opportunity to testify before the May 1, 2002 Subcommittee on Commercial and Administrative Law legislative hearing on H.R. 4561, the "Federal Agency Protection of Privacy Act." The ACLU appreciates your strong commitment to individual privacy rights and supports your efforts to enact H.R. 4561 into law.

As you requested, I respond to the following questions to help inform legislative action on your legislation and develop a more complete hearing record. Please feel free to include this response in the record of the hearing.

1. How does the Federal Agency Protection of Privacy Act differ from existing federal laws pertaining to privacy?

Under current law, the Privacy Act and other federal statutes govern how the federal government may collect, use and disclose individually identifiable personal information. The Federal Agency Protection of Privacy Act (H.R. 4561) does not create new substantive standards regulating the government's collection, use or disclosure of personal information. Instead, H.R. 4561 simply requires agencies to issue an initial and final privacy impact statement assessing how a particular regulation would affect individual privacy.

2. How does the Federal Agency Protection of Privacy Act encourage federal agencies to consider the privacy impact of proposed rules before they are finalized?

Nadine Strossen President  
National Headquarters 125 Broad Street, New York, NY 10004-2400

Anthony D. Romero Executive Director

Kenneth B. Clark Chair, National Advisory Council

Richard Zeckhauser Treasurer  
(212) 549-2500



H.R. 4561 would require federal agencies to issue privacy impact statements with the rules or regulations they propose. Sections 2(a) and (b) of the bill would require federal agencies to issue initial and final privacy impact analyses whenever the agency is required under the APA or other federal law to publish a general notice of proposed rulemaking, including interpretative rules involving tax laws. Based on these provisions, agencies would be required to consider the privacy impact up front and consider less intrusive, equally effective policy alternatives before they make a final decision on a regulation.

By requiring privacy impact statements, the bill would encourage agencies to develop a systematic means for reviewing how a particular regulation would affect individual privacy. In addition, such statements would put the public on notice about the choices federal agencies are making about the use and disclosure of individually identifiable information and give the public a carefully limited chance to participate in those decisions.

The legislation, however, would not give an individual the power to force an agency to adopt a particular alternative. The final privacy impact analysis requires agencies to articulate the available policy options and state why one alternative was selected over the others. But, the bill does not require the agency to adopt the alternative that is least intrusive on privacy.

### 3. How important is the judicial review provision contained in this legislation?

The judicial review provision is an essential component of the legislation. Without this provision, agencies would not be accountable for compliance with the requirements of the bill and individual privacy would continue to be an afterthought in the development of federal policy. The history of the Regulatory Flexibility Act ("RFA") illustrates exactly why judicial review is so important. The RFA was enacted in 1980, but for years federal agencies avoided meaningful implementation of the law by failing to consider less burdensome policy alternatives and attaching boilerplate language to proposed rules in place of the required impact statements. In response, as part of the broader Contract with America, Congress enacted the Small Business Regulatory Enforcement Fairness Act ("SBREFA") and established judicial review provisions in the RFA. Pub.L. 104-121. The findings of the bill noted the requirements of the RFA "have too often been ignored by government agencies." *See also* House Report 104-500, Providing for the Consideration of H.R. 3136, the Contract with America Advancement Act of 1996 (explaining that the SBREFA's judicial review provision "gives teeth to current law").

H.R. 4561 adopts essentially the same judicial review provisions included in the RFA. The bill limits judicial oversight to review of agency compliance with the procedures related to the final privacy impact statement. It does not provide individuals a right to sue over substantive decisions the agency makes in the final regulation.



4. Is the Regulatory Flexibility Act a good model for this legislation?

Yes. H.R. 4561 is modeled after the Regulatory Flexibility Act ("RFA"). 5 U.S.C. §601 seq. For over twenty years, the RFA has required agencies to consider the needs and concerns of small business whenever they engage in rulemaking subject to the notice and comment requirements of the Administrative Procedure Act ("APA") or other federal law. This bill adopts requirements almost identical to those found in the RFA. Instead of assessing the impact on small business, however, the agency analyses would assess the impact of a regulation on individual privacy. The legislation also includes the same waivers available under the RFA. Privacy impact statements would not be required when emergencies make compliance "impracticable."

5. Would H.R. 4561 impose burdensome procedural obligations on federal agency rulemaking?

No. The bill is not overly burdensome and would not hinder the efficiency or functioning of federal agencies. The legislation only applies to rulemaking, not to the vast amount of administrative action that falls outside the formal rulemaking process, including adjudication, informal action, and guidance. Law enforcement agencies would continue to be able to investigate crimes and track down criminals just as they do under current law. In addition, a privacy impact analysis would only be required if a rulemaking is required in the first place. The APA includes exceptions that exempt certain agency functions from the rulemaking process altogether, including when rulemaking procedures are "impracticable, unnecessary, or contrary to the public interest."

6. Currently, are the privacy implications of rules noticed for public comment adequately considered?

No. There is no current federal law that requires agencies to consider the impact of a proposed rule on individual privacy. As a result, federal agencies consistently fail to consider the impact of federal policy on individual privacy. For example, in 1998, pursuant to the Bank Secrecy Act and other federal law, each of the bank regulatory agencies published parallel "Know Your Customer" ("KYC") regulations to facilitate the filing of suspicious activity reports, an element of the agency's broader anti-money laundering initiative. Most banking institutions already had adopted KYC programs voluntarily. The proposed regulations, however, would have mandated uniform standards across the banking industry.

The purpose of the KYC regulations was to facilitate the financial institution's compliance with anti-money laundering laws and to protect the financial institution from accidentally facilitating criminal activity. The impact of the regulation, however, would have been to require banks to track innocent individuals in their day to day financial

transactions and collect and track an enormous amount of personal financial information through federal databases. The Treasury Department was overwhelmed by almost 300,000 comments on “Know Your Customer” regulations because the agency failed to consider the privacy implications of tracking customers’ routine banking activities and reporting personal financial information to the government before issuing the rule. As a result, the agency was forced to retreat and withdraw the rule.

As demonstrated by the proposed KYC regulations, federal regulators can be forced back to the drawing board, wasting significant federal resources, when they fail to consider the privacy impact of a rule up front.

7. Would the Federal Agency Protection of Privacy Act address this concern?

Yes. The legislation would require agencies to consider both a proposed rule’s impact on individual privacy and less intrusive policy alternatives *before* the publication of the final rule.

The “initial privacy impact analysis” would be published with the agency’s proposed rulemaking and the public would have an opportunity to comment on the privacy impact statement and the underlying regulation. The contents of the impact analysis would include an assessment of the extent to which the proposed rule will impact individual privacy interests including: 1) what personally identifiable information is to be collected, and how it is to be collected, maintained and used; 2) whether and how individuals can access the personal information that pertains to them; 3) how the agency prevents the information collected one purpose from being used for another purpose; and 4) what security safeguards are in place to prevent unauthorized disclosure of personal information. Most importantly, the agency must describe alternatives to the proposed rule that accomplish the policy objective but minimize impact on individual privacy.

A “final privacy impact analysis” would be issued with the final rule or regulation. This final privacy impact statement would include the same categories of information as the initial impact statement. In addition, the agency would have to explain the steps it has taken to minimize the “significant” privacy impact on individuals, including the factual, policy and legal reasons for selecting the alternative adopted in the final rule and why the other alternatives were rejected. The final privacy impact statement would also summarize the significant issues raised in the public comments.

8. H.R. 4561 requires agencies to periodically review the rules that impact personal privacy. Do technological changes and changing public values make this periodic review necessary?

Yes. Agencies should periodically review the rules that impact personal privacy because there may be new opportunities to improve the privacy of individually identifiable information.

Section 2(e) of H.R. 4561 would require a periodic review of rules that have a "significant privacy impact on individuals, or a privacy impact on a substantial number of individuals" to determine whether a rule can be amended or rescinded to minimize an adverse privacy impact. Such review is required to take place within ten years of the date of enactment of the regulation. Agencies are also required to publish plans for these reviews in the Federal Register and invite public comment on whether the rule should be rescinded or amended.

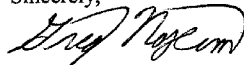
Section 2(e) would provide an important check on agencies' decisions regarding individually identifiable information by requiring them to reconsider past policy choices in light of new information. Advances in technology may provide agencies with new privacy protective policy alternatives. For example, the Bush administration's medical records privacy regulation has created a new market for software and other information technology that limit access to sensitive data, strip out identifiers when they are unnecessary to a particular health care function, and enhance the confidentiality of personal health information through better computer security.

In addition, agencies may want to reconsider their policy choices altogether given changed public values. Generally, the public is very concerned about the privacy of their personal information. As previously noted, the federal government was overwhelmed by almost 300,000 comments on KYC regulations that would have undermined the privacy of financial information. An April 2001 study conducted by the American Society of Newspaper Editors found that 50% were "very concerned" and 30% were "somewhat" concerned that government might violate their personal privacy.

Even after September 11, the public continues to value individual privacy. For instance, immediately after the attacks, a Harris Poll found that 68% of Americans supported a national ID system. A Washington Post study conducted in November 2001 found that only 44% of Americans supported national ID. A poll released in March 2002 by the Gartner Group found that 26% of Americans favored a national ID, and that 41% opposed the idea. Popular support for other surveillance technologies has declined as well. Section 2(e) would ensure that agencies re-consider whether a particular policy choice made in a particular historical context continues to be in the best interest of the public.

Thank you for the opportunity to contribute this additional material to the hearing record. Please contact me at (202) 675-2326 with any questions.

Sincerely,



Gregory T. Nojeim  
Associate Director and Chief Legislative Counsel



Your Source for Privacy Policy from a Free-market, Pro-technology Perspective

May 24, 2002

The Hon. Bob Barr, Chairman  
Subcommittee on Commercial and Administrative Law  
House Judiciary Committee  
U.S. House of Representatives  
2138 Rayburn House Office Building  
Washington, D.C. 20515-6216

Dear Chairman Barr:

Thank you for the opportunity to testify at the May 1 hearing on H.R. 4561, the "Federal Agency Protection of Privacy Act." I have received your May 10 letter posing additional questions for the hearing record. Below, I have copied your questions, then offered my responses. I hope they usefully inform your consideration of the legislation and the privacy issue in general.

Sincerely,

James W. Harper  
Editor  
Privacilla.org

**1. In your testimony, you stress the difference between personal information obtained by the government and that collected by private actors. Why is it important the government and private sectors be treated differently?**

One of the least recognized elements in current privacy debates is the profound difference between governments and the private sector in how they come to privacy. Businesses and governments are alike in that they thrive on the use of information about people. They differ in important ways, however — ways that change how they use the

information they collect. Radically different incentives affect how governments and businesses collect, use, and store personal information about consumers and citizens, and the two operate in entirely different legal regimes as well.

To businesses, information is a scarce resource that must be paid for one way or another. Businesses may lose customers if they ask for too much information. They seek plenty of information from and about customers, but not so much information, or such sensitive information, that consumers will refuse to transact with them. Governments, on the other hand, can demand information on tax forms, on applications for licenses and benefits, and in numerous other ways without losing 'customers' if they collect too much. Without market incentives to limit their data collection, governments will tend to collect more information than necessary and appropriate.

Unlike businesses, governments do not lose the value of information they hold if they abuse it. A business that loses, gives away, or sells information often reduces the value of that information. Competitors may use it to win customers from the company that generated or collected it, for example. A government, on the other hand, may share all the information it has without reducing its ability to carry out its missions.

If a business uses information in a way that is offensive, it may lose customers and the confidence of investors. As we have seen several times in the recent past, companies may suffer bad public relations because of their information practices, and they may suffer dramatic losses in sales and market capitalization. A government may make offensive uses of information without reducing its ability to function, its ability to collect taxes, or its ability to collect more information.

So, where a business must make tactful and intelligent use of scarce information, a government has few similar incentives. This has dramatic consequences for how the two operate when it comes to protecting privacy, and how they should be treated in terms of regulation.

The fact that governments collect information using the force of law cannot be emphasized strongly enough. When a government agency or program needs personal information, that information will be collected. Individuals have no choice in the matter. This is not the case with businesses that, one way or another, must bargain for the information they want.

An important upshot of this is that consumers are more often allowed to remain anonymous or use fake names when dealing with businesses. As long as one is not committing fraud, the penalty for lying about one's identity to a business may be that a transaction is not completed. When dealing with government, however, anonymity or pseudonymity is often impossible, illegal, or, at the very least, suspicious.

Accountability in government gives rise to privacy problems not found in the business world, as well. The public can and should have access to information that governments

collect because this helps keep governments accountable and because the information was collected using public funds. Open records, a hallmark of open government, may mean that information citizens have been compelled to disclose becomes public. Databases held by businesses, on the other hand, are not available to the public on anything near similar terms. Market conditions apply to their sharing of data. This makes it easier for consumers to demand and receive privacy protections, though the process is never perfect.

In lieu of a healthy system of incentives, governments respond to a patchwork of privacy laws imposed on themselves. These laws do not evolve and respond to change as contract rights do, and as the privacy torts can in common law courts. Government privacy practices move in fits and starts as new uses of information expose loopholes in government privacy protections. The Federal Agency Protection of Privacy Act is such a measure — badly needed because of new public awareness of government threats to privacy.

Because governments are only subject to the laws they make for themselves, information held by governments — even if confidential “by law” — is not as well protected as information held under similar restrictions by businesses. Governments can change the laws that apply to information they hold — and sometimes ignore the laws — without suffering significant adverse consequences. Businesses can not. When governments make objectionable uses of information, there is no higher authority to which aggrieved citizens can appeal. This justifies much more restriction on governments’ access to personal and private information.

## **2. Why is it necessary to place additional safeguards on the collection and distribution of information by the government?**

As discussed above, governments have unique powers to take and use information about people. These represent threats to privacy, civil liberties, and various other interests. We have a great deal to be proud of in the United States because our government characteristically acts with restraint, but there are still many examples where it has acted without sufficient regard for privacy and civil liberties.

One notorious example is internment of Americans of Japanese ancestry during World War II. The United States government used information gathered by the Census Bureau to help round up these Americans. Census Bureau employees opened their files and drew up detailed maps that showed where Japanese Americans were located and how many were living in given areas. Nearly 112,000 people were captured and sent to internment camps during this period.

Privacy invasions and abrogation of civil liberties are not just an artifact of difficult historical times. In 1976, the U.S. Senate’s Select Committee to Study Governmental Operation With Respect to Intelligence Activities (known as the “Church Committee”)

found substantial overreaching in the exercise of domestic surveillance. It established that the targets of intelligence activity in the United States ranged far beyond persons who could properly be characterized as enemies of freedom. Domestic surveillance extended to a wide array of citizens engaging in lawful activity.

In 1997, Congress and the public discovered a practice at the Internal Revenue Service known as file “browsing.” Thousands of IRS employees had access to the files of American taxpayers thanks to a nationwide IRS database. Though there have always technically been rules against browsing those files, the IRS had done little to prevent employees from looking up private information about celebrities, neighbors, ex-spouses, and so on.

In each of these examples, the people wronged received tardy or anemic justice, if any at all. Victims of these types of invasions have relatively little recourse against the government. This necessitates preventative safeguards on collection and distribution of information by governments that would not be appropriate for the private sector. This is not intended as a slight to the beneficent motives of public servants and government programs.

In addition to preventing privacy violations and threats to civil liberties, limiting the collection of information by governments fosters the autonomy and individuality of the American people. People define themselves by exercising power over information about themselves. A free country does not require people to justify the choices they make about what information they share and what they hold close. (This does not mean that public policy should shield people from the costs of their choices.) Our default should be to limit the amount of personal information that governments collect.

American privacy allows our many cultures and subcultures to define for themselves how personal information moves in the economy and society. Collection and distribution of information by the government interferes with the decisions individual citizens would make about what information they share and on what terms. As much as this is an ethereal point, it is an important one about the kind of country we are.

**3. Last year, Privacilla.org issued a report indicating federal agencies routinely exchange personal information among each other. Is this a growing trend? Do any limitations exist on intergovernmental transfer of personal information?**

In March 2001, Privacilla issued a report entitled: *“Privacy and Federal Agencies: Government Exchange and Merger of Citizens’ Personal Information is Systematic and Routine.”* In it, we reported that federal agencies begin a new information-sharing program under the Computer Matching and Privacy Protection Act more than once every two weeks. This is a small subset of the new uses agencies regularly make of personal information.

Though empirical evidence lacks, exchange of personal information by federal agencies does seem to be growing. Computerized databases are increasing in number and size, and standardized formats are making it easier to share data. Many new responsibilities given to federal agencies by Congress require sharing of data, either directly or as the best means to carry out and monitor federal programs. This is why the Federal Agency Protection of Privacy Act is so very timely.

There are few limits on intergovernmental sharing of data. The Privacy Act and the Computer Matching and Privacy Protection Act merely require notice in the *Federal Register* before new “routine use” of information is made or before a computer matching program is initiated. This is the lowest of hurdles, intended to inform rather than impede.

In the Privacy Act, there are limits on what uses can be made of information after it has been shared. Such limits may also exist in the organic laws under which information sharing is often carried out. These go to important non-privacy values like fairness and due process. Limitations on transfer per se are few because, in the past, the advancement of particular government programs has usually taken precedence over abstractions like privacy. The Federal Agency Protection of Privacy Act would help prevent this omission in the future.

#### **4. Do ongoing government efforts to merge data among federal agencies raise significant privacy concerns?**

Rarely is any one exchange of data by federal agencies a significant privacy concern. Taken separately, each is too small to object to on the basis of privacy. And, of course, nearly all new and revised uses of citizens’ personal information are instituted for beneficent purposes like doling out entitlements, managing programs, collecting debts, and investigating malfeasance.

It is the cumulative exchange, merger, and use of personal data across the government that raises privacy concerns. This is why the Federal Agency Protection of Privacy Act will improve consideration of privacy in our public policy. It will allow Congress, the press, and the public to observe the cumulative loss of privacy we suffer due to the scores of new programs and regulations that rely on personal information. With that knowledge, we will all be better equipped to determine the scope, structure, and direction of federal programs and regulations.

Returning to the definition of privacy proffered in testimony submitted for the hearing: Privacy is a subjective condition that individuals enjoy when two factors are in place — legal ability to control information about oneself, and exercise of that control consistent with one’s interests and values.



When government agencies are merging personal data, individual Americans — the subjects of this data — have no effective power to stop it. And they are never in a position to legally opt-out of programs that require data about them. The first factor in privacy is absent. It may be said that information in the hands of government is categorically *unprivate* because individual citizens have no legal power to prevent collection and use of information about themselves.

**5. Why do most government databases eventually wind up being used for purposes inconsistent with their creation?**

It may not be the case that government databases are used for purposes inconsistent with their creation. Rather, they are used for purposes consistent with their creation *plus* many other purposes as well.

One example is the National “New Hires” Database. The Personal Responsibility and Work Opportunity Reconciliation Act of 1996 required the Secretary of Health and Human Services to develop a National Directory of New Hires. This directory is a database of information on all newly hired employees, quarterly wage reports, and unemployment insurance claims in the United States. This is a great deal of personal financial information about American citizens.

The purpose of this new database was entirely laudable — helping states locate parents who have skipped out on their child support obligations. All databases are created for laudable purposes. But they have clear tendencies to grow and adopt new uses, uses which, at some point, may vary dramatically from their original purposes.

Already, the National Directory of New Hires has been expanded to track down defaulters on student loans. Additional expansions have been proposed in successive Congresses, including proposals to give state unemployment insurance officials access to the database.

Databases are useful tools. They are attractive for policy-makers in Congress and federal agencies who want to do creative new things to improve existing government functions and programs. New uses of databases that advance government programs are often, unfortunately, a retreat for personal privacy.

**6. You suggest Fair Information Practices is an ideologically-laden approach to privacy, making no distinction between the government and private industry. Please explain.**

Past studies of privacy have failed to recognize the distinctions between government and the private sector that was articulated in response to the first question above.

In the early 1970s, for example, a committee called “The Secretary's Advisory Committee on Automated Personal Data Systems” within the Department of Health, Education, and Welfare did a seminal study of record keeping practices in the computer age. The intellectual content of its report, commonly known as the “HEW Report,” formed much of the basis of the Privacy Act of 1974. The report dealt extensively with the use of the Social Security Number as the issues stood at that time. (And it shows that concerns about information practices are not as new as we may think.) The report did not distinguish terribly well between private- and public-sector institutions. Scholarship like Public Choice Theory, developed and refined over the years since then, has highlighted the importance of these differences.

The HEW Report recommended a number of information practices, calling them “Fair Information Practices.” The concept remains widely discussed today, but almost 30 years after conception many versions of ‘Fair Information Practices’ are problematic in application and not widely adopted.

‘Fair Information Practices’ do form the basis of 1980 guidelines issued by the Organization for Economic Cooperation and Development, a Paris-based international bureaucracy, and the European Union’s Data Privacy Directive. Happily, the United States is learning from the experience of its friends in Europe. The directives in Europe have empowered government bureaucrats while limiting the ability of European businesses to serve consumers. The experience of Europe does not suggest a path for the United States to follow.

The American tradition of limited government protects privacy somewhat in the public sphere, while market-driven privacy protections appear to be outstripping the European regulatory model. American firms increasingly must have information practices that please consumers. If they do not, they are punished when consumers abandon their products or investors lose confidence in their futures. This means that the great majority of Americans will get a desirable mix of privacy protection, convenience, security, customization, and other interests from our businesses. Europeans may well bristle with privacy “rights,” but when it comes to actual privacy, they may be worse off than Americans.

The “Fair Information Practices” also tend to bring in a variety of other important information policies, such as security, fairness, and enforcement. Each such policy is complex and deserving of careful, separate analysis. Some of these policies are inconsistent with others. As was noted in the testimony submitted for the hearing, the Federal Agency Protection of Privacy Act deals with several separate information policy issues. Because it only requires notice of such things, its requirements do no harm.

Advocates who push an entire menu of ‘Fair Information Practices’ on either government or the private sector may be using the privacy debate to pursue a variety of policies that add up to ideology. There is nothing wrong with ideology per se — Privacilla.org wears a “free-market, pro-technology” stance on its sleeve. We believe

that competition among companies to serve consumers is the best way to discover and deliver privacy on the terms they desire. There are honestly held views to the contrary. Some of them buy strongly into whole-cloth adoption of various ‘Fair Information Practices.’ These deserve careful consideration — and often rejection on the merits.

**7. Will the Federal Agency Protection of Privacy Act provide sufficient public notice concerning a rule’s potential impact on personal privacy?**

Through *Federal Register* publication, the Federal Agency Protection of Privacy Act will provide some notice concerning a rule’s effects on personal privacy. *The Federal Register* remains a publication of almost perfect obscurity to the vast majority of Americans, of course. They should receive better notice. Thanks to the Web and e-mail, for example, federal agencies could directly notify many citizens about how proposed regulations would affect uses of personal information about them. Furthermore, affirmative limits on data collection would be preferable to mere notice.

But the Federal Agency Protection of Privacy Act takes measure of the fact that information practices in federal agencies have developed over decades and they can not change quickly. It is a moderate step on the path toward more robust notice and more affirmative privacy protections.

Required to examine and discuss proposed rules in terms of privacy, agencies will naturally tend to build privacy considerations into their rulemakings. Thus, the Federal Agency Protection of Privacy Act will have an indirect impact that protects privacy by reducing ever-so-slightly the range of personal information practices agencies adopt by regulation.

The Federal Agency Protection of Privacy Act will also reflect back to Congress how its own actions affect privacy. As agencies will surely make clear in their Privacy Impact Assessments — and they should — many privacy impacts are either directly or indirectly mandated by statute. This, too, will improve the deliberation that goes into public policies.

Governments are the most serious threats to privacy, so one can not call a moderate step like the Federal Agency Protection of Privacy Act entirely “sufficient.” The legislation is a sufficient start toward further discussion of the privacy issue and greater protection for privacy from government.

**8. Other than the changes you suggest in your testimony, how else might the legislation be improved?**

The Federal Agency Protection of Privacy Act would improve the consideration of privacy in our public policy if it were passed as introduced or with the few amendments that have been suggested.

